UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA

Formas Quadráticas e Testes de Primalidade em "Disquisitiones Arithmeticae"

Francisco Manuel Albuquerque Picado

Mestrado em Matemática

Dissertação orientada por:
Prof. Doutor Pedro Jorge Santos Freitas

2021

Resumo

Em 1801, o matemático alemão Carl Friedrich Gauss publica *Disquisitiones Arithmeticae*, uma das primeiras obras da área da Teoria dos Números, com o objetivo de reunir os resultados desta disciplina e expandir o seu âmbito.

Na secção entitulada *Duae methodi, numeros compositos a primis dignoscendi, illorumque factores inuestigandi*[1], artigos 329 – 334, Gauss concebeu um teste de primalidade baseado na teoria desenvolvida nos capítulos precedentes, nomeadamente os resíduos quadráticos e as formas quadráticas binárias.

Na presente dissertação, apresentam-se estes métodos de Gauss acompanhados dos resultados necessários para os entender plenamente.

Como nota final, mostram-se exemplos da sua aplicação e uma implementação física deste método sugerida por Gauss, usando um dispositivo baseado no que é comummente designado *'pauzinhos de gelado'*.

Palavras-chave: resíduos quadráticos, formas quadráticas binárias, números primos, números compostos

[1] Proposta de tradução: "Dois métodos para distinguir números compostos de números primos e para determinar os seus fatores"

Abstract

In 1801, the German mathematician Carl Friedrich Gauss published *Disquisitiones Arithmeticae*, one of the first books in the field of Number Theory, aiming to gather the results of this new subject and expand on their scope.

In section *Duae methodi, numeros compositos a primis dignoscendi, illorumque factores inuestigandi*[2], articles 329 – 334, Gauss created a primality test, where he applied some of the theory developed in the previous chapters, such as quadratic residues and binary quadratic forms.

In this dissertation, we present these methods created by Gauss along with the main results needed to fully comprehend them.

As a final note, we show some examples of their application and a physical device based on suggestions by Gauss, using what is commonly referred to as *'popsicle sticks'*.

KEYWORDS: quadratic residues, binary quadratic forms, prime numbers, composite numbers

[2]Suggested translation: "Two methods to distinguish between composite numbers from primes and for determining their factors"

Agradecimentos

O filósofo madrileno José Ortega y Gasset disse na sua obra *Meditaciones del Quijote*, de 1914, "Eu sou eu e a minha circunstância.". Logo, todos os que passaram por mim contribuiram para uma percentagem não-nula desta dissertação. No entanto, ainda que o conjunto destas pessoas tenha cardinalidade finita, esta é de uma ordem de grandeza demasiado elevada para enumerar toda a gente, pelo que me limito a agradecer a quem mais me impactou e espero que os demais não se sintam menosprezados, pois estarão tão presentes quanto a minha memória conseguirá mantê-los.

Começo por agradecer à Universidade de Lisboa, pelas oportunidades que me proporcionou ao longo destes anos. Tanto pessoal como academicamente, um agradecimento muito especial é devido ao meu orientador, o professor Pedro Jorge Freitas, pela sugestão do tema, pela sua atenção, pelo seu cuidado e pela sua paciência, mesmo com os atrasos e metamorfoses pelas quais esta dissertação passou. Devo também um agradecimento ao professor Paulo Almeida por ser prestável e pelos seus conhecimentos que muitas vezes me mostraram um caminho a seguir. Agradeço à Universidade de Aveiro, pelo conhecimento que me transmitiu na minha curta passagem, em especial à Inês Costa, ao Gabriel Cardoso, e à Mónica Celis. O trabalho desta última iniciou um rumo a seguir nesta dissertação. Um agradecimento especial é devido ao professor Andrew Granville pelo voto de confiança em mim depositado aquando de me transmitir o seu trabalho em curso sobre o *Disquisitiones Arithmeticae*. Por me ter levado para a *Dixtior Consulting Lda.*, agradeço ao Miguel Barros, pois acabou por influenciar o lado computacional desta dissertação. À Mariana Pereira, agradeço por me ter ajudado com a estrutura da tese. Também agradeço aos meus professores Maria Antónia Camões, Mário Calado, João Rangel de Lima e Luísa Leite, os quais contribuiram para que pudesse acarinhar a matemática, em vez de a ver como um bicho de sete cabeças.

Um agradecimento muito especial devido à Lia Malato Leite, cuja amizade, companhia e apoio desde o início do dia até às longas horas da madrugada foram essenciais para a conclusão desta dissertação. Os seus conhecimentos de LaTeX foram um contributo valioso para a apresentação deste trabalho. Pelo seu apoio e companheirismo, agradeço à Rita Beja e ao João Becho. Sem eles, o primeiro ano da licenciatura em Matemática não teria sido tão memorável. Agradeço à Inês Valente, pelos passeios, fotos e pela citação do início desta secção. Agradeço à Marta Chmielewska por me acompanhar enquanto ambos escreviamos as nossas dissertações de mestrado. Agradeço ao *Circo Matemático* e aos seus membros, por continuarem a mostrar-me uma maneira mais leve e divertida de encarar a Matemática. Pela revisão do texto, agradeço

à Isabel Leite. Por me ajudarem a testar o código presente no anexo D.2.3 agradeço ao Diogo Caridade, ao João Becho, ao Francisco Bento, ao Francisco Caldeira, à Diana Ferreira, ao Rodrigo Girão Serrão, ao Pedro Machado e à Lia Malato Leite.

Acabo por agradecer à minha familia, no geral. Em particular, agradeço profundamente à minha mãe Maria João e ao meu pai Rui que sempre me apoiaram e encorajaram a que fizesse o que mais desejava. Pelo amor, apoio e dedicação que me transmitiram, não poderia estar mais grato. Em segundo lugar, preciso de agradecer à minha avó Zaida por toda a sua atenção e carinho, e por me ter deixado 'acampar' em sua casa durante largas temporadas de forma a trabalhar nesta dissertação. Em sua casa, comecei e completei o rascunho final deste texto, e convido o leitor a que reflita na bonita capicua que isto inspira. Finalmente, quero agradecer aos meus irmãos Nuno e Duarte, pelo seu companheirismo, e ao meu padrasto Rui e à minha madrasta Paula, por toda a ajuda prestada.

Em conclusão, gostaria de deixar uma pequena nota pelo meu avô 'Manel'. Ele era surdo e comunicámos por cartas durante anos. Numa das cartas escreveu "Espero ver-te um dia a aplicar as Matemáticas pelo Mundo.". Acho que finalmente posso dizer que o estou a fazer.

Índice

Lista de Figuras

Lista de Tabelas

Glossário

primo Um número natural p é primo se tem dois, e só dois, divisores positivos distintos: 1 e p.

monoide Um conjunto com uma operação binária associativa e que tem elemento neutro.

grupo Um conjunto com uma operação binária associativa, que tem elemento neutro, e em que cada elemento é invertível.

quadrado Um número inteiro q é um número quadrado caso $q = k^2$, para certo k inteiro. Estes números costumam ser chamados 'quadrados perfeitos'. Caso contrário, dizemos que q é um número não-quadrado.

livre de quadrados Um número inteiro é livre de quadrados quando não é divisível por nenhum número quadrado.

Nomenclatura

Conjuntos

$\mathbb{N}$ conjunto dos números naturais, assumimos que $\mathbb{N} = \{0, 1, 2, \ldots\}$.

$\mathbb{N}_p$ conjunto dos números naturais maiores ou iguais a p

$\mathbb{Z}$ conjunto dos números inteiros

$\mathbb{Q}$ conjunto dos números racionais

$\mathbb{R}$ conjunto dos números reais

$\mathbb{C}$ conjunto dos números complexos

Símbolos

$\equiv$ congruência, i.e., $a \equiv b \pmod{n}$ significa "a e b são congruentes módulo n", para a, b inteiros e n um inteiro não-nulo.

$\mid$ divide, i.e., $a \mid b$ significa "a divide b", para a, b inteiros.

$\lceil x \rceil$ o menor inteiro maior ou igual a x

$\lfloor x \rfloor$ o maior inteiro menor ou igual a x

$\leftrightarrow_P$ equivalência própria entre matrizes, i.e., $A \leftrightarrow_P B$ significa que A e B são propriamente equivalentes.

$\leftrightarrow$ equivalência entre matrizes, i.e., $A \leftrightarrow B$ significa que A e B são equivalentes.

A^{-1} matriz inversa de uma matriz A

A^T matriz transposta de uma matriz A

$\odot$ composição de formas quadráticas, i.e., $F \odot G$ significa "composição de F com G".

t.q. tal que

Funções

det dada uma matriz A, denotamos o seu determinante por $\det(A)$.

mdc dados 2 inteiros m e n, denotamos o máximo divisor comum entre eles por $\text{mdc}(m, n)$.

Introdução

A presente dissertação tem por objetivo a obtenção do grau de Mestre em Matemática pela Universidade de Lisboa.

É um dado bastante aceite dentro da comunidade matemática que a Matemática não se cinge aos cálculos. A sua natureza e a abstração que lhe subjaz nos tempos atuais deixam pouca margem para dúvidas. No entanto, nem sempre foi assim. A execução de cálculos aritméticos já ocupou o tempo de tantos ilustres matemáticos no passado e, para os ajudar nesta árdua tarefa, foram surgindo tecnologias de computação como os ábacos (ca. 5500 a.C), a Pascalina (séc. XVII), o computador clássico (séc. XX), e o computador quântico (séc. XXI), com o objetivo de automatizar estes processos. Não obstante, mesmo com todos estes avanços tecnológicos, a Aritmética e a Teoria dos Números continuam a encerrar importantes problemas em aberto à comunidade matemática. Alguns destes problemas são de particular relevância para áreas como a Criptografia, pois é a sua dificuldade de resolução que é a base de certos criptosistemas. Para o efeito, podemos citar o problema do "logaritmo discreto", o qual é um elemento importante da troca de Diffie-Hellman, ou ainda o problema da "fatorização de números inteiros", o qual é parte do criptosistema de Rabin e do famosíssimo criptosistema RSA. Esta dissertação aborda principalmente o último problema, a fatorização de números inteiros.

Em 1801, Carl Friedrich Gauss publicou o seu *magnum opus*, *Disquisitiones Arithmeticae* (DA), uma obra monumental, responsável por fundar a área da Teoria dos Números e por contribuir para as bases da Álgebra moderna. Ao longo dos tempos, o DA foi sendo editado e traduzido para vários idiomas como o Francês, o Inglês, o Alemão, o Catalão e o Castelhano. Poucos trabalhos sobre esta obra foram realizados em língua portuguesa, o que, aliado à necessidade de modernizar a notação e o raciocínio de Gauss, motivou a presente dissertação.

Na secção composta pelos artigos numerados entre 329 e 334 de DA figura um processo de fatorização de números inteiros, processo este que não dependia de identidades polinomiais e que foi pioneiro na sua época. Na presente dissertação procuramos expor os trabalhos de Gauss constantes dos artigos 329, 330, 331, 332, a fim de apresentar e estudar a fundo este processo, que, neste âmbito, batizamos de *Crivo Gaussiano*, por analogia a algoritmos como o Crivo de Eratóstenes.

Apresentamos os conceitos do DA, de forma a requerer poucos conhecimentos prévios. Este trabalho está estruturado do seguinte modo:

Capítulo 1 – Recapitulação da teoria dos resíduos quadráticos, os quais serão um elemento-chave para os estudos de Gauss. Concluímos com o enunciado e a demonstração da identidade de Brahmagupta e do Teorema Chinês dos Restos.

Capítulo 2 – Apresentação das bases teóricas do Crivo Gaussiano e uma das suas partes que pode ser totalmente compreendida após leitura do capítulo 1. Para o efeito, desenvolvemos um estudo autónomo de certas equações quadráticas, o qual decorre diretamente de duas recomendações ligeiras da parte de Gauss.

Capítulo 3 – Exposição de parte dos estudos de Gauss sobre o tema das formas quadráticas binárias, das suas propriedades básicas à composição de formas, passando pela Teoria de Caracteres. Expomos sobretudo os trabalhos diretamente relacionados com o Crivo Gaussiano. Esta é a parte mais extensa da dissertação.

Capítulo 4 – Exemplificação do uso da teoria presente no capítulo 3 no âmbito do Crivo Gaussiano.

Capítulo 5 – Apresentação das relações entre os vários temas desenvolvidos nos capítulos precedentes. Após estudarmos o lado puramente teórico da geração de resíduos quadráticos nos capítulos anteriores, começamos por apresentar as bases da fatorização de inteiros e concluímos com a descrição de uma possível técnica e respetiva implementação para fatorizar dois números inteiros, um escolhido por Gauss e outro escolhido pelo mestrando.

Após o texto principal, apresentamos 5 anexos, por forma a complementá-lo e enriquecer a sua leitura (Anexos A-E).

Anexo A – Exposição de uma aplicação artesanal dos trabalhos de Gauss.

Anexo B – Descrição de alguns critérios de divisibilidade.

Anexo C – Apresentação de duas técnicas para o cálculo manual de raízes quadradas de números inteiros.

Anexo D – Exposição de código programado na linguagem de programação *Python* com o objetivo de facilitar os cálculos. Aqui figuram implementações da maioria dos algoritmos descritos ao longo da dissertação.

Anexo E – Apresentação de parte da história da Teoria dos Números desde a Antiguidade ate à publicação do DA.

Ao longo deste texto, o tratamento dos trabalhos de Gauss baseou-se predominantemente na tradução da sua obra em língua castelhana ([Gau95]), tendo também sido consultada a sua edição original, em Latim ([Gau01]), e a sua edição em língua inglesa ([Gau86]). A adaptação do DA feita pelo professor Granville ([Gra]) foi também estudada com o mesmo fim, sobretudo nos algoritmos de redução de formas quadráticas. Sempre que nos referirmos à obra de Gauss, o leitor poderá confirmar a informação em qualquer uma das quatro obras citadas.

Todas as citações presentes no texto foram traduzidas para a língua portuguesa, podendo o leitor consultar a sua versão original em nota de rodapé. Quaisquer lacunas ou incorreções constantes da presente dissertação são da minha total responsabilidade.

Capítulo 1

Conceitos de Teoria dos Números

Este capítulo cumpre o propósito de descrever o universo a que dizem respeito os estudos desenvolvidos por Gauss e caracterizar os objetos mais essenciais a todo o trabalho de Gauss, os resíduos quadráticos. Apresentaremos a maioria dos resultados sem demonstrações, pois só necessitaremos do seu enunciado. Os leitores interessados poderão encontrar demonstrações em [Ros11], [AN17], [Gau95]. Gauss começa assim o prefácio do *Disquisitiones Arithmeticae*:

> *"As investigações contidas neste volume pertencem à parte da Matemática que trata dos números inteiros, por vezes, frações, mas nunca de irracionais"* ([Gau01], p. VII)[1].

Portanto, o objeto de estudo desta teoria são os elementos de $\mathbb{Z}$ mas, por vezes, necessitaremos de recorrer a $\mathbb{Q}$. Comecemos por apresentar umas noções de base.

Teorema 1.1 (Teorema Fundamental da Aritmética)
Qualquer $N \in \mathbb{Z} \setminus \{0, \pm 1\}$ admite uma representação única como um produto de potências de primos distintos, a menos da ordem dos fatores,

$$N = \pm p_0^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m},$$

sendo p_i números primos distintos, $\alpha_i \in \mathbb{N}_1$ e $m \in \mathbb{N}$.

Definição 1.2 (Fatorização)
Uma FATORIZAÇÃO de um número inteiro N é uma representação de N como produto de números inteiros menores ou iguais a N. Estes números inteiros são denominados FATORES. Caso os fatores sejam todos números primos, então são chamados FATORES PRIMOS e dizemos que esta é uma FATORIZAÇÃO EM PRIMOS.

Neste momento, estamos preparados para tratar um dos objetos mais importante em toda esta dissertação.

[1] No original: "Disquisitiones in hoc opere contentae ad eam Matheseos partem pertinent, quae circa numeros integros versatur, fractis plerumque, surdis sempre exclusis."

1.1 Resíduos Quadráticos

1.1.1 Propriedades gerais

Definição 1.3 (Resíduo Quadrático)
Sejam $a, n \in \mathbb{Z} \setminus \{0\}$. Consideremos a congruência: $x^2 \equiv a \pmod{n}$. Se esta for possível, a é um RESÍDUO QUADRÁTICO MÓDULO n. Caso contrário, a é um NÃO-RESÍDUO QUADRÁTICO MÓDULO n.

Observação 1.4 (Notação)
No decurso deste texto, a denominação "RESÍDUO QUADRÁTICO MÓDULO n" poderá ser abreviada para "RESÍDUO QUADRÁTICO MOD n", "RESÍDUO QUADRÁTICO", ou somente "RESÍDUO". A expressão recorrente "RESÍDUO QUADRÁTICO DE n" tem o mesmo significado e é decalcada diretamente da obra estudada, [Gau95].

Exemplo 1.5
Considerando congruências módulo 10*, a tabela abaixo mostra os possíveis valores de* x^2*.*

$x \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$x^2 \pmod{10}$	**0**	**1**	**4**	**9**	**6**	**5**	**6**	**9**	**4**	**1**

Tabela 1.1: Quadrados perfeitos módulo 10

Daqui se conclui que:

1. $x^2 \equiv 2^2 \equiv 4 \pmod{10}$ *é possível, logo* 4 *é resíduo quadrático* mod 10*.*
2. $x^2 \equiv 5 \pmod{10}$ *é possível, logo* 5 *é resíduo quadrático* mod 10*.*
3. $x^2 \equiv 7 \pmod{10}$ *é impossível, logo* 7 *é não-resíduo quadrático* mod 10*.*

Proposição 1.6 (Sobre o número de resíduos quadráticos)
Seja $n \in \mathbb{Z} \setminus \{0\}$, o número de resíduos quadráticos módulo n não excederá $\frac{n}{2} + 1$ caso n seja par e não excederá $\frac{n+1}{2}$ caso n seja ímpar.

Demonstração. Seja $a \in \mathbb{Z}$ e $n \in \mathbb{Z} \setminus \{0\}$ t.q. $a < n$. Em módulo n, sabemos que $(n-1)^2 \equiv 1^2$, $(n-2)^2 \equiv 2^2, \ldots$ Como tal, ao elevarmos ao quadrado os elementos de $\{0, 1, 2, ..., n-1\}$ obteremos vários valores repetidos e, quando muito, teremos os valores acima referidos.

Q.E.D.

Observação 1.7
Usando um argumento semelhante e o lema 1.31, conseguimos demonstrar que teremos exatamente $\frac{n-1}{2}$ resíduos quadráticos, caso n seja um número primo ímpar.

Exemplo 1.8
Tomemos a congruência $x^2 \equiv 4 \pmod{10}$*. Vendo os dados anteriores,* $2^2 \equiv 4 \pmod{10}$*, o que permite concluir que* 2 *é solução da congruência. Analogamente, como* $(10-2)^2 = 8^2$*, podemos concluir que* $8^2 \equiv 4 \pmod{10}$*. Assim,* $x^2 \equiv 4 \pmod{10}$ *tem as duas soluções:* 2 *e* 8*.*

Observação 1.9
Em particular, $x^2 \equiv 1 \pmod{n}$ é possível, com soluções $-1, 1$. Deste modo, 1 é sempre resíduo quadrático módulo n.

Observação 1.10 (Produto de resíduos quadráticos)
O produto de resíduos quadráticos é também um resíduo quadrático.

Demonstração. Suponha-se que são possíveis as congruências

$$x^2 \equiv a \pmod{n} \qquad \text{e} \qquad y^2 \equiv b \pmod{n},$$

com soluções x_0 e y_0, respetivamente. Então, $z^2 \equiv ab \pmod{n}$ também será possível, com solução $x_0 y_0$.

Q.E.D.

Com as últimas duas observações, fica provado:

Corolário 1.11
Seja $n \in \mathbb{Z} \setminus \{0\}$. O conjunto dos resíduos quadráticos módulo n forma um monoide comutativo com a operação de multiplicação.

Para tratar mais propriedades destes resíduos quadráticos, será prudente dividir por casos. Trataremos primeiro o caso em que o módulo é um número primo.

1.1.2 Números primos

Definição 1.12 (Símbolo de Legendre)
Seja $p \geqslant 3$ um número primo, $a \in \mathbb{Z}$. O SÍMBOLO DE LEGENDRE vem definido por:

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} 0, & \text{caso } p \mid a. \\ 1, & \text{caso } a \text{ seja um resíduo quadrático mod } p. \\ -1, & \text{caso } a \text{ seja um não-resíduo quadrático mod } p. \end{cases}$$

Observação 1.13 (Notação)
No decurso do texto seguinte, referir-nos-emos ao símbolo $\left(\frac{a}{p}\right)$ por extenso como "Símbolo de Legendre de a". Quando for necessário, especificaremos "Símbolo de Legendre de a módulo p".

Exemplo 1.14
Seja $p = 7$ primo. Como $3^2 \equiv 2 \pmod{7}$, vem que $x^2 \equiv 2 \pmod{7}$ é possível, donde

$$\left(\frac{2}{7}\right) = 1.$$

No entanto, $x^2 \equiv 3 \pmod{7}$ é impossível. Logo,

$$\left(\frac{3}{7}\right) = -1.$$

Proposição 1.15 (Critério de Euler)
Seja $p \geqslant 3$ um número primo, $a \in \mathbb{Z}$.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Corolário 1.16 (Alguns símbolos rápidos)
Seja p um número primo ímpar.

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}, \qquad \left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Observação 1.17 (Frações módulo n)
Ao longo desta dissertação, denotaremos $\frac{p}{q} \pmod{n}$ com o significado de $pq^{-1} \pmod{n}$. Esta expressão só se usa caso q seja invertível módulo n, e neste caso, q^{-1} é o seu inverso módulo n.

Demonstração. Segue-se, tanto quanto sabemos, uma prova original para o símbolo de Legendre de 2. Seja p um número primo ímpar e consideremos o fatorial de $\frac{p-1}{2}$:

$$\left(\frac{p-1}{2}\right)!. \tag{1.1}$$

Através de manipulações algébricas, chegamos ao seguinte:

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv \left(\frac{p-1}{2}\right)\left(\frac{p-3}{2}\right)(...)\left(\frac{p-(p-4)}{2}\right)\left(\frac{p-(p-2)}{2}\right) \pmod{p} \\ &\equiv (2^{-1})^{\frac{p-1}{2}}(p-1)(p-3)(...)(p-(p-4))(p-(p-2)) \pmod{p} \\ &\equiv (2^{-1})^{\frac{p-1}{2}}(-1)\cdot(-3)\cdot(...)\cdot 4\cdot 2 \pmod{p}.\end{aligned}$$

Neste produto, teremos sensivelmente metade dos números entre 1 e $\frac{p-1}{2}$ com sinal negativo. Caso $\frac{p-1}{2}$ seja par, teremos $\frac{p-1}{4}$ sinais negativos. Caso $\frac{p+1}{2}$ seja par, teremos $\frac{p+1}{4}$ sinais negativos. Tomando o sinal de $p \pm 1$ de forma a que $\frac{p\pm1}{4} \in \mathbb{Z}$, segue que:

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv (2^{-1})^{\frac{p-1}{2}} \cdot (-1)^{\frac{p\pm1}{4}} \cdot 1\cdot 2\cdot 3\cdot 4\cdot(\ldots)\left(\frac{p-1}{2}\right) \pmod{p} \\ &\equiv (2^{-1})^{\frac{p-1}{2}} \cdot (-1)^{\frac{p\pm1}{4}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}.\end{aligned}$$

Devido a que $\left(\frac{p-1}{2}\right)! \not\equiv 0 \pmod{p}$, temos que $\operatorname{mdc}\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$. Como tal, segue que:

$$1 \equiv (2^{-1})^{\frac{p-1}{2}} \cdot (-1)^{\frac{p\pm1}{4}} \pmod{p}.$$

Caso $4 \mid p+1$, vem que $\frac{p-1}{2}$ é ímpar. Logo $(-1)^{\frac{p-1}{2}} = (-1)$. Donde,

$$(-1)^{\frac{p+1}{4}} = \left((-1)^{\frac{p-1}{2}}\right)^{\frac{p+1}{4}} = (-1)^{\frac{p^2-1}{8}}.$$

Considerando que $(2^{-1})^{\frac{p-1}{2}} = \left(2^{\frac{p-1}{2}}\right)^{-1}$ segue-se:

$$1 \equiv \left(2^{\frac{p-1}{2}}\right)^{-1} \cdot (-1)^{\frac{p^2-1}{8}} \pmod{p} \iff 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

O caso $4 \mid p-1$ é análogo. Pelo Critério de Euler, segue que $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}}$.

Q.E.D.

Observação 1.18
Estes símbolos podem ser mais facilmente calculados, fazendo as seguintes divisões em casos:

1. Caso $p \equiv 1 \pmod 4$, então $\left(\frac{-1}{p}\right) = 1$ e, caso $p \equiv 3 \pmod 4$, então $\left(\frac{-1}{p}\right) = -1$.
2. Caso $p \equiv \pm 1 \pmod 8$, então $\left(\frac{2}{p}\right) = 1$ e, caso, $p \equiv \pm 3 \pmod 8$, então $\left(\frac{2}{p}\right) = -1$.

Exemplo 1.19
Seja $p = 7$ primo. Calculando o símbolo de Legendre de 2 módulo 7, vem

$$\left(\frac{2}{7}\right) \equiv 2^{\frac{7-1}{2}} \equiv 2^3 \equiv 1 \pmod 7.$$

Corolário 1.20
Seja $p \geqslant 3$ um número primo e $a, b \in \mathbb{Z}$. Da proposição 1.15, podemos concluir o seguinte:

1. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
2. Se $a \equiv b \pmod p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Observação 1.21
Sendo p primo, podemos traduzir a primeira condição do corolário acima dado por:

1. O produto de 2 resíduos quadráticos módulo p é um resíduo quadrático módulo p.
2. O produto de 2 não-resíduos quadráticos módulo p é um resíduo quadrático módulo p.
3. O produto de um não-resíduo quadrático módulo p com um resíduo quadrático módulo p é um não-resíduo quadrático módulo p.

Observação 1.22
O inverso de um resíduo quadrático é também um resíduo quadrático. Do mesmo modo, o inverso de um não-resíduo quadrático é um não-resíduo quadrático.

Demonstração. Seja $a \in \mathbb{Z} \setminus \{0\}$ e p um número primo. Suponhamos que $\text{mdc}(a, p) = 1$ e que $aa^{-1} \equiv 1 \pmod p$. Segue então que,

$$\left(\frac{a}{p}\right)\left(\frac{a^{-1}}{p}\right) = \left(\frac{aa^{-1}}{p}\right) = \left(\frac{1}{p}\right) = 1 \iff \left(\frac{a}{p}\right) = \left(\frac{a^{-1}}{p}\right).$$

Q.E.D.

Assim, demonstrámos o próximo resultado.

Corolário 1.23
O conjunto dos resíduos quadráticos positivos em módulo primo tem a estrutura de um grupo comutativo com a operação de multiplicação.

Segue-se a exposição da Lei da Reciprocidade Quadrática, um teorema tão importante para Gauss que este publicou seis demonstrações do mesmo em vida e outras duas foram encontradas postumamente, em apontamentos.

Teorema 1.24 (Lei da Reciprocidade Quadrática)
Sejam p, q números primos ímpares. Então,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Observação 1.25
A primeira demonstração de Gauss aparece na secção IV de [Gau01]. É demasiado densa para ser apresentada aqui. Outros matemáticos como Eisenstein e Zolotarev simplificaram o trabalho de Gauss, com novas demonstrações. Tal excede os nossos propósitos para este teorema, pelo que omitimos a sua prova e deixamo-la para consulta do leitor em obras como [Ros11] e [Gau95].

Exemplo 1.26
Considerem-se os primos 7 e 61, e é preciso calcular

$$\left(\frac{7}{61}\right).$$

Aplicando a Lei da Reciprocidade Quadrática múltiplas vezes e o corolário 1.20, vem:

$$\begin{aligned}\left(\frac{7}{61}\right) &= \left(\frac{61}{7}\right)(-1)^{\frac{7-1}{2} \cdot \frac{61-1}{2}} = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) \\ &= \left(\frac{7}{5}\right)(-1)^{\frac{7-1}{2} \cdot \frac{5-1}{2}} = \left(\frac{7}{5}\right) \\ &= \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.\end{aligned}$$

É uma aplicação corrente usar este teorema para se saber para que primos q é um certo primo p resíduo quadrático. Vejamos um par de exemplos.

Exemplo 1.27
5 é um resíduo quadrático de que primos p? Ou seja, para que primos p se tem

$$\left(\frac{5}{p}\right) = 1?$$

Aplicando a Lei da Reciprocidade Quadrática, vem:

$$\left(\frac{5}{p}\right) = 1 \iff \left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2} \cdot \frac{5-1}{2}} = 1 \iff \left(\frac{p}{5}\right) = 1.$$

Deste modo, aplicando as propriedades do símbolo de Legendre, vem que $p \equiv 1, 4 \pmod 5$. *Isto significa que 5 será um resíduo quadrático em qualquer primo da forma* $5k + 1$ *ou* $5k + 4$.

Exemplo 1.28
3 é um resíduo quadrático de que primos p? Ou seja, em que primos p se tem

$$\left(\frac{3}{p}\right) = 1?$$

Uma vez que 3 é um número primo, temos que $\left(\frac{3}{3}\right) = 0$ pois 3 divide 3. Supondo agora que $p > 3$, podemos aplicar a Lei da Reciprocidade Quadrática, e vem:

$$\left(\frac{3}{p}\right) = 1 \iff \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = 1 \iff \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = 1.$$

Como o símbolo de Legendre toma os valores 1 e -1, o produto na equação anterior apenas pode ser igual a 1 se $\left(\frac{p}{3}\right)$ e $(-1)^{\frac{p-1}{2}}$ forem iguais. Agora é necessário considerar os casos:

$$\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} = 1 \qquad e \qquad \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} = -1.$$

Fazendo uma conta rápida, obtemos que

$$\left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod 3 \qquad e \qquad \left(\frac{p}{3}\right) = -1 \iff p \equiv 2 \pmod 3.$$

Usando as propriedades do símbolo de Legendre de -1 vistas na observação 1.18, consideramos os sistemas:

$$\begin{cases} p \equiv 1 \pmod 3 \\ p \equiv 1 \pmod 4 \end{cases} \qquad e \qquad \begin{cases} p \equiv 2 \pmod 3 \\ p \equiv 3 \pmod 4). \end{cases}$$

Aplicando o Teorema Chinês dos Restos (teorema 1.47), concluímos que $p \equiv 1, 11 \pmod{12}$.

Observação 1.29
Podemos generalizar o que foi feito para primos arbitrários p e q. Em todo o caso, vemos que os primos p dos quais um certo primo q será resíduo quadrático estão sempre em progressões aritméticas da forma $qk + a$ ou $4qk + a$, sendo $\text{mdc}(a, q) = 1$. No caso de 5 foram as progressões da forma $5k + 1$, $5k + 4$; no caso de 3 foram as progressões da forma $4 \cdot 3k + 1$ e $4 \cdot 3k + 11$.

Acabamos a subsecção com alguns resultados sobre os resíduos quadráticos em módulo primo.

Proposição 1.30
Sejam $a \in \mathbb{Z}$ e p um número primo. Caso a congruência $x^2 \equiv a \pmod p$ seja possível, tomemos x_0 uma sua solução tal que $0 \leqslant x_0 < p$. Então, $(x_0 + pt)^2 \equiv a \pmod p$, para qualquer $t \in \mathbb{Z}$.

Lema 1.31
Sejam $a \in \mathbb{Z}$ e p um número primo. Se a congruência $x^2 \equiv a \pmod p$ for possível, com a solução x_0, então a congruência só admite as soluções distintas x_0 e $p - x_0$ em módulo p.

Proposição 1.32
Sejam $m, n \in \mathbb{N}_1$ e p um número primo ímpar t.q. $m \leqslant n \leqslant 2m$. Então, a é resíduo quadrático módulo p^m se e só se a é resíduo quadrático módulo p^n.

Demonstração. Começamos pela implicação trivial e apenas depois a implicação restante.

($\Longleftarrow$) Caso a seja resíduo quadrático módulo p^n, significa que, para certo $x \in \mathbb{Z}$, $p^n \mid x^2 - a$. Como $p^m \mid p^n$, então $p^m \mid x^2 - a$. Logo, a é resíduo quadrático módulo p^m.

($\Longrightarrow$) Suponhamos que $x_0^2 \equiv a \pmod{p^m}$. Vamos construir uma nova solução x_1 que verifica $x_1^2 \equiv a \pmod{p^{2m}}$. Tomemos $x_1 \equiv x_0 \pmod{p^m}$, ou seja, $x_1 = x_0 + tp^m$, para certo $t \in \mathbb{Z}$. Isto significa que $x_1^2 = x_0^2 + 2tx_0p^m + t^2p^{2m}$ e assim,

$$x_1^2 \equiv x_0^2 + 2tx_0p^m \pmod{p^{2m}}.$$

Sabemos que $x_0^2 \equiv a \pmod{p^m}$, logo $p^m \mid a - x_0^2$. Como $\mathrm{mdc}(2x_0, p^m) = 1$, vem que p não divide $2x_0$ e assim $2x_0$ é invertível módulo p^{2m}. Denotemos este inverso por $\frac{1}{2x_0}$.
Tomamos então $t = \frac{1}{2x_0}\frac{a-x_0^2}{p^m}$ e concluimos que $x_1^2 \equiv a \pmod{p^{2m}}$. Como $p^n \mid p^{2m}$, também temos que $x_1^2 \equiv a \pmod{p^n}$.

Q.E.D.

1.1.3 Números compostos

Quando o módulo é um número composto, não há tanta estrutura entre os resíduos quadráticos. Sobretudo porque agora não é garantida a existência de inverso módulo n. Isto será de suma importância para as conclusões finais.

Observação 1.33 (Resíduos quadráticos em módulo composto)
Sendo n um número ímpar composto, é necessário estabelecer paralelos no que concerne a natureza de resíduos quadráticos módulo n.

1. O produto de resíduos quadráticos é um resíduo quadrático.

2. O produto de não-resíduos quadráticos é de natureza incerta.

   Exemplo 1.34
   Pondo $n = 21$, as congruências $x^2 \equiv 2 \pmod{21}$ e $x^2 \equiv 5 \pmod{21}$ são impossíveis e também o é $x^2 \equiv 2 \cdot 5 \equiv 10 \pmod{21}$. No entanto, $x^2 \equiv 11 \pmod{21}$ não é possível e $x^2 \equiv 2 \cdot 11 \equiv 22 \pmod{21}$ é possível.

3. O produto de um resíduo quadrático com um não-resíduo quadrático é de natureza incerta.

   Exemplo 1.35
   Pondo $n = 21$, a congruência $x^2 \equiv 2 \pmod{21}$ é impossível. Deste modo, as congruências $x^2 \equiv 4 \pmod{21}$ e $x^2 \equiv 9 \pmod{21}$ são possíveis. No entanto, $x^2 \equiv 2 \cdot 4 \equiv 8 \pmod{21}$ não é possível e $x^2 \equiv 2 \cdot 9 \equiv 18 \pmod{21}$ é possível.

No entanto, ainda que haja menos estrutura no conjunto dos resíduos quadráticos, podemos adaptar a proposição 1.30 e obter o seguinte enunciado.

Observação 1.36
Caso a congruência $x^2 \equiv a \pmod{n}$ seja possível, tomemos x_0 uma solução tal que $0 \leqslant x_0 < n$. Então, teremos $(x_0 + nt)^2 \equiv a \pmod{n}$, para qualquer $t \in \mathbb{Z}$.

Para os nossos estudos seguintes, podemos generalizar o Símbolo de Legendre para que este seja aplicável a números ímpares não necessariamente primos.

Definição 1.37 (Símbolo de Jacobi)
Sejam $a \in \mathbb{Z}$ e $n \geqslant 3$ um número ímpar tal que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, onde p_m são números primos ímpares distintos e $\alpha_i \in \mathbb{N}_1$. O SÍMBOLO DE JACOBI vem definido por:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_m}\right)^{\alpha_m},$$

sendo $\left(\frac{a}{p_m}\right)$ o símbolo de Legendre correspondente.

As próximas propriedades enunciadas podem ser deduzidas através da definição do Símbolo de Jacobi usando as propriedades análogas do Símbolo de Legendre.

Proposição 1.38
Seja $n \geqslant 3$ um número ímpar e $a, b \in \mathbb{Z}$.

1. $\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$.
2. Se $a \equiv b \pmod{n}$, então $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

Do mesmo modo, também temos fórmulas fechadas para calcular este símbolo mais facilmente.

Proposição 1.39
Seja $n \geqslant 3$ um número ímpar.

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \qquad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

Uma vez que a condição de primalidade de p não importa para as condições da observação 1.18, é também possível generalizá-la para o símbolo de Jacobi.

Observação 1.40
Tomando n um número ímpar,

1. Caso $n \equiv 1 \pmod 4$, então $\left(\frac{-1}{n}\right) = 1$ e, caso $n \equiv 3 \pmod 4$, então $\left(\frac{-1}{n}\right) = -1$.
2. Caso $n \equiv \pm 1 \pmod 8$, então $\left(\frac{2}{n}\right) = 1$ e, caso, $n \equiv \pm 3 \pmod 8$, então $\left(\frac{2}{n}\right) = -1$.

Teorema 1.41 (Lei da Reciprocidade Quadrática)
Sejam $n, m \in \mathbb{N}_1$ ímpares t.q. $\text{mdc}(n, m) = 1$. Então,

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) \cdot (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

No entanto, ainda que espelhe muitas das propriedades já vistas para o símbolo de Legendre, este símbolo não é fidedigno no que toca a avaliar se a congruência $x^2 \equiv a \pmod{n}$ é possível.

Exemplo 1.42
Seja $N = 21 = 3^1 \cdot 7^1$. *Temos que*

$$\left(\frac{-1}{21}\right) = \left(\frac{-1}{3}\right)^1 \left(\frac{-1}{7}\right)^1 = (-1) \cdot (-1) = 1.$$

Admita-se que $x^2 \equiv -1 \pmod{21}$ *é possível para certo número inteiro* x*. Então,* $21 \mid x^2+1$*. Como* $21 = 3 \cdot 7$*, segue-se que* $3 \mid x^2+1$ *e* $7 \mid x^2+1$*. Deste modo, têm de ser possíveis estas duas congruências,*

$$x^2 \equiv -1 \pmod{3} \qquad e \qquad x^2 \equiv -1 \pmod{7}.$$

Pelas contas anteriores do símbolo de Legendre de -1 *módulo* 3 *e módulo* 7*, vem que ambas as congruências são impossíveis. Assim, não existe nenhum número inteiro* x *nestas condições e a congruência original não pode ser possível.*

Este fenómeno pode ser explicado pelo próximo teorema, crucial a esta dissertação. O seu nome curioso deve-se ao facto de ser apresentado no artigo 105 da obra estudada, [Gau95].

Teorema 1.43 (Artigo 105, DA)
Sejam $n, m \in \mathbb{N}_1$ t.q. m divide n. Se a é resíduo quadrático módulo n, então a será resíduo quadrático módulo m.

Demonstração. Suponhamos que a é resíduo quadrático de n, ou seja, $x^2 \equiv a \pmod{n}$ é possível. Assim, $n \mid x^2 - a$. Como $m \mid n$, temos que $m \mid x^2 - a$. Ou seja, $x^2 \equiv a \pmod{m}$ é possível. Este raciocínio é aplicável a qualquer divisor de n, em particular, aos seus divisores primos.

Q.E.D.

Porém, a afirmação recíproca deste teorema ser-nos-á mais útil, pelo que a transcrevemos abaixo.

Corolário 1.44 (Artigo 105, DA)
Sejam $n, m \in \mathbb{N}_1$ t.q. m divide n. Se a é não-resíduo quadrático módulo m, a é não-resíduo quadrático módulo n

Em conclusão, para que a seja resíduo quadrático módulo n, o teorema anterior indica que terá de ser resíduo quadrático módulo p_i, para qualquer p_i divisor primo de n. Baseando-nos nesta conclusão, mostramos adiante o caso geral que explica o exemplo 1.42.

Sejam $a \in \mathbb{Z}$ e $n \geqslant 3$ um número ímpar tal que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, onde p_m são números primos ímpares distintos e $\alpha_i \in \mathbb{N}_1$. Queremos calcular o Símbolo de Jacobi $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_m}\right)^{\alpha_m}$. Suponhamos que temos uma parcela deste produto, $\left(\frac{a}{p_i}\right)^{\alpha_i}$, na qual α_i é ímpar. Pelas propriedades do Símbolo de Legendre, segue que,

$$\left(\frac{a}{p_i}\right)^{\alpha_i} = -1 \Longrightarrow \left(\frac{a}{p_i}\right) = -1.$$

Logo, a é não-resíduo quadrático módulo p_i, e assim é não-resíduo quadrático módulo n, pelo corolário 1.44. Suponhamos que temos várias parcelas $\left(\frac{a}{p_i}\right)^{\alpha_i}$ tais que $\left(\frac{a}{p_i}\right)^{\alpha_i} = -1$ e α_i ímpar. Nesta circunstância, se $2 \mid \alpha_1 + \alpha_2 + \ldots + \alpha_m$, teremos um número par de α_i ímpares. Logo, no produto final, teremos uma quantidade par de parcelas iguais a -1, o que torna o produto final igual a 1. Provámos então que é possível que o símbolo de Jacobi de a módulo n seja igual a 1, mesmo que a seja um não-resíduo quadrático módulo n. O Símbolo de Jacobi não nos dá certezas devido a um problema de paridade. No entanto, analogamente a este raciocínio, podemos concluir a seguinte observação.

Observação 1.45 (O Símbolo de Jacobi não devolve falsos negativos)
Sejam $a \in \mathbb{Z}$ e $n \in \mathbb{N}_3$, número ímpar. Caso $\left(\frac{a}{n}\right) = (-1)$, então $x^2 \equiv a \pmod{n}$ é impossível.

Devido à sua utilidade para os resultados seguintes, apresentamos as identidades de Brahmagupta com uma demonstração.

Lema 1.46 (Identidades de Brahmagupta)
Sejam $\alpha, \beta, \gamma, \delta, \varepsilon \in \mathbb{C}$. Então:

$$(\alpha^2 - \varepsilon\beta^2)(\gamma^2 - \varepsilon\delta^2) = (\alpha\gamma + \varepsilon\beta\delta)^2 - \varepsilon(\alpha\delta + \beta\gamma)^2,$$

$$(\alpha^2 + \varepsilon\beta^2)(\gamma^2 + \varepsilon\delta^2) = (\alpha\gamma - \varepsilon\beta\delta)^2 + \varepsilon(\alpha\delta + \beta\gamma)^2.$$

Podemos fazer um simples cálculo usando álgebra linear o que também pode conferir alguma compreensão, além de nos parecer mais elegante.

Demonstração. Considerando as matrizes:

$$A = \begin{pmatrix} \alpha & \varepsilon\beta \\ \beta & \alpha \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} \gamma & \varepsilon\delta \\ \delta & \gamma \end{pmatrix}.$$

O seu produto é:

$$AB = \begin{pmatrix} \alpha\gamma + \varepsilon\beta\delta & \varepsilon(\alpha\delta + \beta\gamma) \\ \alpha\delta + \beta\gamma & \alpha\gamma + \varepsilon\beta\delta \end{pmatrix}.$$

Pelas propriedades do determinante de uma matriz, vem que $\det(AB) = \det(A) \cdot \det(B)$.
Isto demonstra a primeira identidade, já que

$$\det(A) = (\alpha^2 - \varepsilon\beta^2), \qquad \det(B) = (\gamma^2 - \varepsilon\delta^2), \qquad \det(AB) = (\alpha\gamma + \varepsilon\beta\delta)^2 - \varepsilon(\alpha\delta + \beta\gamma)^2.$$

A segunda identidade pode ser provada do mesmo modo, trocando o sinal às entradas na posição (1,2) em cada uma das matrizes A e B.

Q.E.D.

Para facilitar a leitura desta dissertação, deixamos expresso o Teorema Chinês dos Restos.

Teorema 1.47 (Teorema Chinês dos Restos)
Sejam $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ e $n_1, n_2, \ldots, n_k \in \mathbb{N}_1$ coprimos dois a dois. Então, o sistema de congruências

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \cdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

tem uma única solução mod $N = n_1 \cdots n_k$.

Demonstração. Como a prova é construtiva, vamos apenas transcrever a sua solução. Tomamos $N = n_1 n_2 \cdots n_k$, $N_i = \frac{N}{n_i}$ e y_i tal que $N_i y_i \equiv 1 \pmod{n_i}$ para $1 \leqslant i \leqslant k$. Então, a única solução módulo N vem dada por $X = a_1 N_1 y_1 + \cdots + a_k N_k y_k$.

Q.E.D.

Capítulo 2

Busca de resíduos quadráticos: Primeira Parte

Com a teoria exposta até agora, já é possível apresentar uma primeira parte dos métodos de Gauss, e como tal, talvez seja prudente ver uma aplicação para que esta não chegue tarde demais. Sem querer adiantar demasiado, a ideia de Gauss será usar os resíduos quadráticos de um número inteiro N por forma a encontrar os seus fatores primos. Deste modo, o objetivo deste capítulo é expor os fundamentos das técnicas de Gauss para calcular resíduos quadráticos de N. No final, mostramos um algoritmo baseado nas recomendações de Gauss.

2.1 Busca de resíduos quadráticos

No artigo 332 de DA, Gauss expõe três métodos para encontrar resíduos quadráticos de N. O que veremos de seguida é o primeiro método de Gauss para se encontrar estes resíduos quadráticos. Os dois métodos restantes baseiam-se em características das formas quadráticas binárias que apresentaremos no capítulo seguinte. Para todos os métodos será necessário ter presente o lema seguinte, o qual será sobretudo útil para simplificar os resíduos já obtidos.

Lema 2.1 (Lema da Eliminação do Quadrado)
Sejam $b, k, N \in \mathbb{Z} \setminus \{0\}$. Suponhamos que $\text{mdc}(k, N) = 1$ e bk^2 é resíduo quadrático módulo N. Então, b será resíduo quadrático módulo N.

Demonstração. Suponhamos que $x^2 \equiv bk^2 \pmod{N}$ é possível. Como $\text{mdc}(k, N) = 1$, k é invertível módulo N. Portanto, seja m o seu inverso[1]. Vem então:

$$\begin{aligned} x^2 \equiv bk^2 \pmod{N} &\iff x^2m^2 \equiv bk^2m^2 \pmod{N} \\ &\iff (xm)^2 \equiv b(km)^2 \pmod{N} \\ &\iff (xm)^2 \equiv b \pmod{N}. \end{aligned}$$

Ou seja, b também tem de ser resíduo quadrático módulo N.

Q.E.D.

[1] A justificação para o uso desta letra é meramente gráfica. Supusemos que a potência negativa usualmente conotada com o inverso posta em simultâneo com o quadrado tornaria a leitura pesada.

Por esta razão, Gauss afirma que resíduos divisíveis por quadrados grandes são exatamente tão úteis como os resíduos pequenos. Para os métodos de Gauss, desejamos obter resíduos tão pequenos quanto possível. Deste modo, doravante, a nossa análise incidirá sobre os resíduos livres de quadrados. Como o produto de resíduos quadráticos também será um resíduo quadrático, podemos 'forçar' a aparição de resíduos quadráticos divisíveis por quadrados e assim simplificá-los pelo lema 2.1, como vemos no próximo exemplo.

Exemplo 2.2
Suponhamos que $N = 5209$. *Vem que* 5 *é resíduo quadrático módulo* N, *mas também o é* $2 \cdot 3 \cdot 5$. *Logo, o seu produto* $2 \cdot 3 \cdot 5^2$ *é resíduo quadrático módulo* N. *Usando o lema 2.1, como* $\text{mdc}(5, N) = 1$, *vem que* $2 \cdot 3$ *é um resíduo quadrático menor que* $2 \cdot 3 \cdot 5$ *em valor absoluto.*

Este género de simplificações será ferramenta habitual para os métodos de Gauss e estará sempre presente. Gauss apresenta assim o seu primeiro método para encontrar resíduos quadráticos:

> *"O método mais simples e conveniente, para aqueles que adquiriram alguma destreza através do exercício frequente, consiste em decompôr* N *ou um seu múltiplo em duas partes"* ([Gau01], p.583)[2].

A ideia de Gauss não é nem difícil de enunciar, nem difícil de demonstrar. No entanto, será um resultado central a todo o método, e talvez seja boa ideia reservar-lhe uma proposição.

Definição 2.3 (Decomposição)
Seja $N \in \mathbb{Z}$. Chamamos DECOMPOSIÇÃO a uma representação de N como soma de 2 inteiros.

Proposição 2.4 (Proposição da Decomposição)
Consideremos $a, b, k, N \in \mathbb{Z} \setminus \{0\}$. Caso $kN = a + b$, então $-ab$ é resíduo quadrático mod N.

Demonstração. Suponhamos que $kN = a + b$. Então,

$$a + b \equiv 0 \pmod{N} \iff a \equiv -b \pmod{N} \iff a^2 \equiv b^2 \equiv -ab \pmod{N}.$$

Assim, $-ab$ é resíduo quadrático módulo N.

Q.E.D.

Nem todas as decomposições são úteis ou sequer manejáveis. Caso N seja um número bastante grande, haverá bastantes decomposições infrutíferas. Necessitamos de critérios adicionais de forma a otimizar o uso desta proposição. Deste modo, o ilustre matemático faz 2 recomendações:

1. Nas decomposições a procurar, será útil que uma parte ou ambas sejam múltiplas de quadrados.

2. De forma a que b seja tão pequeno quanto possível, a deve ser um múltiplo de um quadrado próximo de kN.

[2]No original: "Methodus simplicissima, iisque, qui per frequentem exercitationem iam aliquam dexteritatem sibi conciliauerunt, commodissima, consistit en eo, vt M aut generalius multiplum quodcunque ipsius M quomodocunque in duas partes decomponatur kM = a + b ..."

Ambas estas recomendações estão presentes nas decomposições que Gauss apresenta e se transcrevem no próximo exemplo. O autor de DA mostra esta panóplia de decomposições sem explicar como as calculou. O que se pretende nesta secção, após o exemplo, é explorar variantes da decomposição presente na proposição 2.4 para obter somas semelhantes.

Exemplo 2.5

Como veremos adiante no capítulo 5, Gauss tem o objetivo de fatorizar o número 997331 *em primos. Sendo assim, como* $998 < \sqrt{997331} < 999$*, é possível calcular*

$$\begin{aligned} 997331 &= 999^2 - 2 \cdot 5 \cdot 67 \\ &= 994^2 + 5 \cdot 11 \cdot 13^2 \\ &= 2 \cdot 706^2 + 3 \cdot 17 \cdot 3^2 \\ &= 3 \cdot 575^2 + 11 \cdot 31 \cdot 4^2 \\ &= 3 \cdot 577^2 - 7 \cdot 13 \cdot 4^2 \\ &= 3 \cdot 578^2 - 7 \cdot 19 \cdot 37 \\ &= 11 \cdot 299^2 + 2 \cdot 3 \cdot 5 \cdot 29 \cdot 4^2. \end{aligned}$$

Consideremos a primeira decomposição: $997331 = 999^2 - 2 \cdot 5 \cdot 67$*. Pela proposição 2.4, viria que* $2 \cdot 5 \cdot 67 \cdot 999^2$ *é resíduo quadrático módulo* 997331*. Como* $\text{mdc}(999, 997331) = 1$*, podemos aplicar o lema 2.1 e considerar somente* $2 \cdot 5 \cdot 67$*. Analogamente, podemos criar a próxima tabela.*

Decomposição	Resíduos
$999^2 - 2 \cdot 5 \cdot 67$	$2 \cdot 5 \cdot 67$
$994^2 + 5 \cdot 11 \cdot 13^2$	$-5 \cdot 11$
$2 \cdot 706^2 + 3 \cdot 17 \cdot 3^2$	$-2 \cdot 3 \cdot 17$
$3 \cdot 575^2 + 11 \cdot 31 \cdot 4^2$	$-3 \cdot 11 \cdot 31$
$3 \cdot 577^2 - 7 \cdot 13 \cdot 4^2$	$3 \cdot 7 \cdot 13$
$3 \cdot 578^2 - 7 \cdot 19 \cdot 37$	$3 \cdot 7 \cdot 19 \cdot 37$
$11 \cdot 299^2 + 2 \cdot 3 \cdot 5 \cdot 29 \cdot 4^2$	$-11 \cdot 2 \cdot 3 \cdot 5 \cdot 29$

Tabela 2.1: Decomposições e resíduos quadráticos de 997331

Usando a observação 1.10, podemos multiplicar alguns destes resíduos para forçar a aparição de um quadrado, como já foi visto. Por exemplo, ao multiplicar o resíduo quadrático $-5 \cdot 11$ *pelo resíduo quadrático* $-2 \cdot 3 \cdot 5 \cdot 11 \cdot 29$ *obtemos o número* $2 \cdot 3 \cdot 29 \cdot (5 \cdot 11)^2$*. Como* $\text{mdc}(20137, 5 \cdot 11) = 1$*, pelo lema 2.1, podemos simplificar o resíduo quadrático e trabalhar apenas com* $2 \cdot 3 \cdot 29$*.*

Estudo sobre a decomposição de N

Até ao final desta secção, veremos um estudo autónomo feito somente a partir das recomendações de Gauss. Acabamos o texto com um processo para obter uma decomposição de N mais vantajosa. Assumimos que $N, k \in \mathbb{N}_1$, pois, caso $kN < 0$, a técnica é análoga. O objetivo é encontrar resíduos quadráticos de N usando a decomposição presente na proposição 2.4:

$$kN = a + b. \tag{2.1}$$

Segundo Gauss, seria bastante útil que o produto de ambas as partes fosse divisível por um número quadrado. Tal se cumpre com a decomposição:

$$kN = x^2 + d. \tag{2.2}$$

Ao decompôr kN desta forma, pela proposição 2.4, $-dx^2$ é um resíduo quadrático de N. Sendo possível aplicar o lema 2.1, concluimos que $-d$ é um resíduo quadrático de N.

Observação 2.6 (Método de Força Bruta)
Sabemos que a equação (2.2) é equivalente à equação $x^2 - kN = -d$. Ou seja, as imagens da função polinomial $x^2 - kN$ serão resíduos quadráticos de N após mudança de sinal. Esta maneira é simples de executar (e pode ser facilmente automatizada), mas pode ser pouco prática dado que é complicado controlar a ordem de grandeza dos resíduos quadráticos.

Vista a observação anterior, o nosso objetivo será lidar com resíduos quadráticos de uma ordem de grandeza o mais pequena possível, logo será conveniente minimizar o valor de d. Para o efeito, isto é equivalente a ter x tão perto de $\sqrt{kN}$ quanto possível. Portanto, para esta primeira decomposição, podemos calcular raízes quadradas de kN e tomar os inteiros mais próximos. Uma vez que de cada equação se extrai duas aproximações inteiras (por excesso e por defeito), teremos sempre dois valores possíveis para d. Ou seja, com k_0, $k_1 \in \mathbb{N}$, procuramos a resolução explicita

$$kN = \left(\lfloor \sqrt{kN} \rfloor\right)^2 + k_0 = \left(\lceil \sqrt{kN} \rceil\right)^2 - k_1. \tag{2.3}$$

Observação 2.7
No Anexo C, exploramos técnicas manuais de modo a obter esta raiz quadrada sem o uso de máquinas, de modo a contextualizar este método com a época de Gauss. Estes não são os únicos processos para calcular a raiz quadrada de um número e deixam-se como recomendação.

Exemplo 2.8
Tomemos $N = 5209$. *Deste modo,* $72 < \sqrt{5209} < 73$. *Usando estes dados, temos que*

$$5209 = 72^2 + 25 = 73^2 - 120.$$

Para aplicar o lema 2.1, após garantir que não há fatores em comum entre 72 *e* N, *concluímos que* -25 *será resíduo quadrático módulo* 5209. *Como* $-25 = (-1) \cdot 5^2$, *podemos aplicar o lema 2.1 novamente após garantir que não há fatores em comum entre* 5 *e* N *e assim eliminamos o quadrado para concluir que* -1 *é resíduo quadrático. Pelo mesmo raciocínio, temos que* 120 *é resíduo quadrático e como* $120 = 2 \cdot 3 \cdot 5 \cdot 2^2$, *podemos reduzi-lo ao resíduo equivalente* $2 \cdot 3 \cdot 5$

De seguida, vamos generalizar esta decomposição de forma a calcular novos resíduos quadráticos. O seu estudo constitui um passo intermédio para estudarmos formas quadráticas binárias. Por agora, estudamos a decomposição

$$ax^2 + cn = kN. \tag{2.4}$$

Para a execução do processo seguinte, é necessário fixar $a, k, n, N \in \mathbb{N}_1$. O objetivo é resolver em ordem a x e a c. No entanto, geralmente, nem sempre há solução para esta equação.

Observação 2.9
Caso existam x e c que verifiquem a equação (2.4), sabemos que $d = \text{mdc}(a, n)$ será um fator de kN. Uma vez que desconhecemos a fatorização de N, pode acontecer que $d \nmid N$ e $d \nmid k$, pelo que a equação pode não ter solução. Para facilitar os cálculos, escolhemos a e n tais que $d = 1$.

A partir da equação anterior, podemos concluir que

$$ax^2 \equiv kN \pmod{n} \iff x^2 \equiv \frac{kN}{a} \pmod{n}. \tag{2.5}$$

Se esta congruência for possível, podemos obter uma condição para o valor de x e isto será útil para os passos seguintes. Apresentamos, de seguida, um possível algoritmo para a sua resolução, tentando minimizar o valor de cn. Suponhamos que queremos uma solução para a equação (2.4), quando $n > 1$, pois o processo já calcula um valor para x quando $n = 1$.

Processo de resolução

1. Começamos por comprovar que a congruência $ax^2 \equiv kN \pmod{n}$ é possível. Se for possível, podemos prosseguir para o próximo passo.

2. De seguida, suponhamos que $n = 1$ e consideremos a decomposição auxiliar mais simples $ax^2 + c = kN$. Procuramos um par (x, c) que verifique esta decomposição.

3. Pelo Algoritmo da Divisão, podemos dividir kN por a, e obteremos uma expressão do género $kN = aq + r$. Como tal, assumindo que $kN = ax^2 + c$, segue-se $ax^2 + c = aq + r$.

4. Deste modo, $ax^2 + c - r = aq$, o que equivale a $x^2 + \frac{c-r}{a} = q$. Esta segunda equação será fulcral para encontrar os resíduos quadráticos pretendidos, pois agora temos um caso semelhante à decomposição (2.2) já estudada.

5. De seguida, para obter o menor valor possível para $\frac{c-r}{a}$, é necessário calcular aproximações inteiras de $\sqrt{q}$. O anexo C tem algumas técnicas úteis para este efeito. Após encontrar x_0 e x_1 aproximações satisfazendo $x_0 < \sqrt{q} < x_1$, obtemos $k_0 \geqslant 0$ e $k_1 \leqslant 0$, temos que

$$x_0^2 + k_0 = q \qquad \text{e} \qquad x_1^2 + k_1 = q.$$

6. Assim, de modo a regressar à decomposição auxiliar, é necessário resolver em ordem a c_i as seguintes equações

$$\frac{c_0 - r}{a} = k_0 \qquad \text{e} \qquad \frac{c_1 - r}{a} = k_1.$$

7. Donde, extraímos

$$c_0 = a \cdot k_0 + r \qquad \text{e} \qquad c_1 = a \cdot k_1 + r.$$

8. Pela proposição 2.4, uma vez que sabemos que

$$a \cdot x_0^2 + c_0 = kN \qquad \text{e} \qquad a \cdot x_1^2 + c_1 = kN,$$

os números $-a \cdot c_i \cdot x_i^2$ serão resíduos quadráticos módulo kN, para $i \in \{0, 1\}$.

9. No final do passo anterior, obtemos decomposições da forma $ax^2+c = kN$, e vamos querer usá-las para obter decomposições da forma $ax^2 + cn = kN$. Para tal, nas decomposições já encontradas, vamos alterar o valor de x_i para encontrar elementos c_i divisiveis por n.

   (a) Nas decomposições auxiliares, $ax^2 + c_i = kN$, caso x_i satisfaça a congruência (2.5), isto significa que $n \mid c_i$. Logo, supondo $c_i = nc_i'$, chegamos a uma decomposição $ax^2 + c_i'n$.

   (b) Caso x_i não satisfaça a congruência (2.5), procuramos novos valores que a satisfaçam. Por facilidade de cálculo, procuramos valores da forma (x_i+l), com $l \in \mathbb{Z}$. De seguida, procuramos valores de l que tornem a seguinte congruência verdadeira,

$$a(x_i + l)^2 \equiv kN \pmod{n}.$$

   Ao termos uma nova solução $x_i + l$ para esta congruência, vem que

$$n \mid a(x_i + l)^2 - kN \iff nu = a(x_i + l)^2 - kN, \text{ para certo } u \in \mathbb{Z}.$$

   Logo, $a(x_i + l)^2 + n(-u) = kN$. Pondo $-u = c_i'$, temos a decomposição desejada.

Após um processo tão detalhado, talvez seja benéfico mostrarmos um exemplo aplicando os processos anteriores.

Exemplo 2.10
Tomando $N = 21037$. Podemos estudar a decomposição:

$$105185 = 5N = 3x^2 + 2c.$$

Pelo algoritmo explicado antes,

1. *A congruência $3x^2 \equiv 5N \pmod 2$ é possível, podemos prosseguir para o próximo passo.*
2. *Consideramos a decomposição auxiliar $5N = 3x^2 + c$.*
3. *Efetuando a divisão por a, neste caso, 3, obtemos $105185 = 3 \cdot 35061 + 2$. Logo, $q = 35061$.*
4. *Podemos reduzir a decomposição auxiliar ao caso mais simples, donde*

$$105185 = 3x^2 + c \iff x^2 + \frac{c-2}{3} = 35061.$$

5. *Calculando $\sqrt{35061}$, obtemos como melhores aproximações:*

$$x_0^2 + 92 = 35061,\ x_0 = 187 \qquad e \qquad x_1^2 - 283 = 35061,\ x_1 = 188.$$

6. *Do mesmo modo:*

$$92 = \frac{c_0 - 2}{3} \qquad e \qquad -283 = \frac{c_1 - 2}{3}.$$

7. *Portanto*

$$c_0 = 3 \cdot 92 + 2 = 278 \qquad e \qquad c_1 = 3 \cdot (-283) + 2 = -847. \tag{2.6}$$

8. *Daqui extraímos as decomposições:*

$$105185 = 3 \cdot 187^2 + 278 \qquad e \qquad 105185 = 3 \cdot 188^2 - 847.$$

Por estas contas obtemos que $-3 \cdot 278 \cdot 187^2$ *e* $3 \cdot 847 \cdot 188^2$ *são resíduos quadráticos módulo* 21037*, pela proposição 2.4. Pelo lema 2.1, podemos simplificar cada resíduo para obter* $-3 \cdot 278$ *e* $3 \cdot 847$*, pois* $\text{mdc}(187, 21037) = \text{mdc}(188, 21037) = 1$*. Este processo pode ser repetido, pois* $847 = 7 \cdot 11^2$ *e* $\text{mdc}(11, 21037) = 1$*, donde* $3 \cdot 847 = 3 \cdot 7 \cdot 11^2$ *reduz-se a* $3 \cdot 7$*.*

9. *Voltando ao caso original* $3x^2 + 2c = 105185$*, recuperemos a congruência (2.5), para testar se os produtos anteriores se podem subdividir mais.*

   (a) *Quanto a* x_0*, temos que* $3 \cdot x_0^2 \equiv 5N \pmod 2$*, pelo que* 2 *é divisor de* c_0*.*

   (b) *Quanto a* x_1*, temos que* $3 \cdot x_1^2 \not\equiv 5N \pmod 2$*. Ou seja,* $2 \nmid c_1$*, como também já vimos. No entanto,* $3 \cdot (x_1 + 1)^2 \equiv 5N \pmod 2$*. Portanto,* $2 \mid 3 \cdot (188 + 1)^2 - 5N$*. Donde,* $l = 1$*. Ou seja,* $3 \cdot 189^2 + 2 \cdot (-989) = 5N$*.*

Nas suas recomendações, Gauss sugeriu que o produto das duas partes da decomposição fosse divisível por um número quadrado. Podemos melhorar a decomposição (2.4) caso consideremos uma decomposição da forma

$$ax^2 + cy^2 = kN. \tag{2.7}$$

Podemos chegar a esta decomposição pegando no processo anterior, mas supondo que n é um quadrado perfeito. No entanto, se tivermos encontrado uma decomposição $ax^2 + cn = kN$, podemos encontrar outra solução w tal que $aw^2 + c'n^2 = kN$. Logo, quereremos encontrar o valor w para o qual se tem $n^2 \mid kN - aw^2$. Portanto, pegamos na congruência (2.5), e procuramos resolver a congruência $aw^2 \equiv kN \pmod{n^2}$. Ou seja,

$$ax^2 \equiv kN \pmod n \longrightarrow aw^2 \equiv kN \pmod{n^2}.$$

Pela observação 1.36 e pela proposição 1.30, sabemos que, para todo o $t \in \mathbb{Z}$, $x + nt$ serão soluções da primeira congruência. Analogamente ao que fizemos na proposição 1.32, podemos calcular um valor de t que satisfaça a congruência

$$a(x + nt)^2 \equiv kN \pmod{n^2}. \tag{2.8}$$

E assim, após algumas manipulações algébricas, obtemos

$$(2anx)t \equiv kN - ax^2 \pmod{n^2}. \tag{2.9}$$

Sendo possível, resolvemos a congruência (2.9) em ordem a t para obter os valores $w = x + nt$ para os quais $n^2 \mid aw^2 - kN$. Assumindo $\text{mdc}(2ax, n) = 1$, esta solução será única módulo n.

Exemplo 2.11
Suponhamos que $N = 21037$. *Queremos encontrar uma decomposição da forma* $x^2 + 5^2c = 3N$, *na qual* $a = 1$, $n = 5$, $k = 5$. *Ao resolver a congruência* $x^2 \equiv 3N \pmod 5$, *obtemos que* $x \equiv 1 \pmod 5$. *Daqui concluimos que existirá* $t \in \mathbb{Z}$, *tal que*

$$(1 + 5t)^2 \equiv 3N \pmod{5^2}.$$

Deste modo, $(1+5t)^2 \equiv 11 \pmod{25}$, *donde concluimos que* $t \equiv 1 \pmod 5$. *Aplicando o algoritmo anterior para* $x^2 + 5c = 3N$, *obtemos que* $251^2 + 5 \cdot 22 = 3N$. *Usando o valor de* t *descoberto, temos que* $3N - (251 + 5 \cdot 1)^2 = -2425 = 5^2 \cdot (-97)$. *A partir de* $251^2 + 110 = 3N$, *obtemos a decomposição* $256^2 - 97 \cdot 5^2 = 3N$, *entre outras.*

Após algumas contas, pudemos compilar os nossos resultados na tabela transcrita abaixo. Esta contém uma coluna com as decomposições encontradas e uma coluna com os resíduos que cada decomposição nos fornecia após todas as simplificações feitas. Reunimos uma seleção dos resíduos mais simples no capítulo 5 para os usar na fatorização deste número.

Decomposição	Resíduos
$145^2 + 3 \cdot 2^2 = 21037$	-3
$146^2 - 31 \cdot 3^2 = 21037$	31
$3 \cdot 83^2 + 370 = 21037$	$-2 \cdot 3 \cdot 5 \cdot 37$
$5 \cdot 65^2 - 2^3 \cdot 11 = 21037$	$2 \cdot 5 \cdot 11$
$205^2 + 7^2 = 2 \cdot 21037$	-1
$251^2 + 5 \cdot 22 = 3 \cdot 21037$	$-2 \cdot 5 \cdot 11$
$256^2 - 97 \cdot 5^2 = 3 \cdot 21037$	97
$324^2 + 11 \cdot 19 = 5 \cdot 21037$	$-11 \cdot 19$
$2 \cdot 230^2 - 615 = 5 \cdot 21037$	$2 \cdot 3 \cdot 5 \cdot 41$
$3 \cdot 188^2 - 847 = 5 \cdot 21037$	$3 \cdot 7$

Tabela 2.2: Decomposições e resíduos quadráticos de 21037

2.2 Efeitos colaterais

No presente capítulo, estudámos representações da forma $ax^2 + cy^2$ para N e seus múltiplos, de forma a encontrar resíduos quadráticos de N. No capítulo 5, veremos como eliminar candidatos a divisores primos do número N em questão usando resíduos quadráticos. No entanto, em virtude das representações estudadas e dos resíduos quadráticos encontrados, pode ser possível usar métodos auxiliares de forma a obter uma fatorização de N em primos, com mais celeridade.

Observação 2.12
De acordo com a definição no início do capítulo, será importante frisar que estes métodos auxiliares servem para facilitar a obtenção de uma fatorização de N em primos, mas não é garantido que a sua aplicação nos mostre N como um produto de números primos instantaneamente.

Comecemos com a representação geral que vimos nas páginas anteriores,

$$ax^2 + cn = kN. \tag{2.10}$$

Propriedades da divisão

Suponhamos que $\text{mdc}(ax^2, cn) = d > 1$ e que $m = \text{mdc}(d, k)$ é tal que $d > m > 1$. Então, pelas propriedades da divisão, N será múltiplo de $\frac{d}{m}$. Como teste suplementar, para certezas totais, convém testar os fatores comuns entre ax^2 e cn.

Fatorização de Euler

A ideia de base deste algoritmo terá sido proposta por Marin Mersenne, mas apenas foi posta em prática por Leonhard Euler. Podemos usar este algoritmo caso encontremos duas representações diferentes de N como soma de quadrados para acelerar a obtenção de uma fatorização de N, como visto em [Ore48].

Tomemos N número ímpar que admite duas decomposições como soma de quadrados:

$$N = a^2 + b^2 = c^2 + d^2.$$

Uma vez que N é ímpar, em cada uma das somas de quadrados, um dos quadrados perfeitos terá de ser par e o outro terá de ser ímpar. Sem perda de generalidade, suponhamos que são ímpares a e c e são pares b e d. Neste caso, teremos $a^2 - c^2 = d^2 - b^2$. Ou seja,

$$(a - c) \cdot (a + c) = (d - b) \cdot (d + b). \tag{2.11}$$

Definindo $k = \text{mdc}(a - c, d - b)$, vem que $a - c = kl$ e $d - b = km$ com $l, m \in \mathbb{N}_1$ e $\text{mdc}(l, m) = 1$. Pelo afirmado anteriormente, $a - c$ e $d - b$ são pares. Substituindo na equação (2.11)

$$kl(a + c) = km(d + b) \iff l(a + c) = m(d + b), \tag{2.12}$$

como l, m são coprimos, $m \mid a + c$, portanto, $a + c = mn$, com $n \in \mathbb{N}_1$. Continuando os cálculos em (2.12), temos $l(mn) = m(d + b) \iff ln = d + b$. Assim, porque $\text{mdc}(l, m) = 1$, podemos concluir que $n = \text{mdc}(a + c, d + b)$. Em conclusão,

$$N = \left(\left(\frac{k}{2}\right)^2 + \left(\frac{n}{2}\right)^2\right) \cdot (m^2 + l^2).$$

Para o verificar, basta aplicar as identidades de Brahmagupta, presentes no lema 1.46,

$$\begin{aligned}(k^2 + n^2) \cdot (m^2 + l^2) &= (km + nl)^2 + (kl - mn)^2 \\ &= ((d - b) + (d + b))^2 + ((a - c) - (a + c))^2 \\ &= 4 \cdot (d^2 + c^2) = 4 \cdot N.\end{aligned}$$

Exemplo 2.13
Seja $N = 2501 = 50^2 + 1^2 = 49^2 + 10^2$. *Considerando os dados anteriores, temos que:*

$$a = 1, \qquad b = 50, \qquad c = 49, \qquad d = 10.$$

Pelo que podemos calcular:

$$a - c = -48, \qquad a + c = 50, \qquad d - b = -40, \qquad d + b = 60.$$

E assim, segue:

$$k = \text{mdc}(a - c, d - b) = 8 \qquad e \qquad n = \text{mdc}(a + c, d + b) = 10.$$

Pela fórmula anteriormente deduzida, sabemos que $\left(\frac{k}{2}\right)^2 + \left(\frac{n}{2}\right)^2$ *é divisor de* N*. Portanto, como*

$$41 = \left(\tfrac{8}{2}\right)^2 + \left(\tfrac{10}{2}\right)^2.$$

Efetuando a divisão, obtemos[3]*:*

$$2501 = 41 \cdot 61.$$

Considerações de Fermat

A partir de um método de fatorização que se atribui a Fermat, podemos acelerar a obtenção de uma fatorização de N, como visto em [AN17].

Seja N o número inteiro a fatorizar e sejam $x, y \in \mathbb{Z}$ t.q.

$$x^2 - y^2 = N.$$

Afigura-se como uma identidade útil neste caso, a fatorização de polinómios

$$x^2 - y^2 = (x - y)(x + y).$$

Portanto, após considerar $a = x - y$ e $b = x + y$, temos que $N = ab$. Deste modo, obtemos uma fatorização de N. No entanto, podemos encontrar a representação seguinte:

$$x^2 - y^2 = kN. \tag{2.13}$$

Neste caso, a técnica anterior não funciona totalmente. Ainda que $x - y$ ou $x + y$ sejam divisores de kN, podem não ser divisores de N. No entanto, terão fatores primos em comum. Assim, podemos considerar $d = \text{mdc}(N, x + y)$, o qual será um fator não trivial de N, caso $k \neq x - y$.

Exemplo 2.14

Vejamos 2 casos que beneficiam grandemente destas considerações auxiliares:

1. *Seja* $N = 2021$*. Como* $N = 45^2 - 2^2$*, vem* $N = (45 - 2)(45 + 2)$*. Logo,* $N = 43 \cdot 47$*.*
2. *Seja* $N = 141467$*. Temos a representação* $3 \cdot 141467 = 655^2 - 68^2$*. Neste caso, podemos considerar* $d = \text{mdc}(141467, 655 + 68) = 241$ *como um fator não-trivial. Este permite-nos concluir que* $141467 = 241 \cdot 587$*.*

[3]Podemos calcular a representação de 61 como soma de quadrados, atendendo ao facto que $61 = m^2 + l^2$, sendo m e l como definidos na dedução da fatorização de Euler. Neste caso $61 = 5^2 + (-6)^2$.

Congruências de quadrados

Também podemos abordar o problema da representação (2.13), focando-nos somente nos resíduos quadráticos. Usando os métodos desta secção, conseguimos obter resíduos quadráticos módulo N bem como uma das suas raízes quadradas. Isto significa que lidamos com congruências

$$x_0^2 \equiv a_0 \pmod{N}, \qquad x_1^2 \equiv a_1 \pmod{N}, \qquad \ldots \qquad x_n^2 \equiv a_n \pmod{N},$$

nas quais, tanto x_i como a_i são conhecidos. Pode acontecer que possamos tomar um subconjunto dos índices $\{i_0, i_1, \ldots, i_l\} \subseteq \{0, 1, \ldots, n\}$ de forma a que

$$a_{i_0} a_{i_1} \ldots a_{i_l} \equiv y_0^2 \pmod{N}.$$

Nesta circunstância, como o produto de resíduos quadráticos é um resíduo quadrático,

$$\begin{aligned}(x_{i_0} x_{i_1} \ldots x_{i_l})^2 \equiv y_0^2 \pmod{N} &\iff (x_{i_0} x_{i_1} \ldots x_{i_l})^2 - y_0^2 \equiv 0 \pmod{N} \\ &\iff N \mid (x_{i_0} x_{i_1} \ldots x_{i_l})^2 - y_0^2\end{aligned}$$

Ou seja, existe $k \in \mathbb{Z} \setminus \{0\}$, tal que $kN = (x_{i_0} x_{i_1} \ldots x_{i_l})^2 - y_0^2$. Agora podemos proceder como já foi estudado e tomar $d = \text{mdc}(x_{i_0} x_{i_1} \ldots x_{i_l} + y_0, N)$. Caso tenhamos que $x_{i_0} x_{i_1} \ldots x_{i_l} - y_0 \neq k$, então d é um fator não trivial de N.

Exemplo 2.15
Podemos tomar o número $N = 2021$.

$$\begin{aligned}2 \cdot 32^2 - 3 \cdot 3^2 = 2021 &\implies 2 \cdot 32^2 \equiv 3 \cdot 3^2 \pmod{2021} \\ &\implies 64^2 \equiv 6 \cdot 3^2 \pmod{2021} \\ &\implies \left(\frac{64^2}{3^2}\right) \equiv 6 \pmod{2021} \\ &\implies 695^2 \equiv 6 \pmod{2021}.\end{aligned}$$

Analogamente, podemos tratar a equação seguinte

$$8 \cdot 19^2 - 3 \cdot 17^2 = 2021 \implies 960^2 \equiv 24 \pmod{2021}.$$

Donde se conclui que

$$(695 \cdot 960)^2 \equiv 270^2 \equiv 12^2 \pmod{2021}.$$

Assim, $d = \text{mdc}(270 + 12, 2021) = 47$*, o qual será um fator não trivial de* 2021.

Pode ser trabalhoso efetuar tanto o cálculo das raízes quadradas dos resíduos quadráticos de N como das raízes apropriadas, pelo que sugerimos cautela no recurso a este método.

Capítulo 3

Formas Quadráticas Binárias

Este capítulo serve o propósito de expor os fundamentos teóricos desenvolvidos por Gauss para se entender as últimas duas técnicas para gerar resíduos quadráticos módulo N, sendo N o número a fatorizar em primos. Neste capítulo, queremos apenas expor e desenvolver os resultados necessários para se entender como usar formas quadráticas binárias para gerar resíduos quadráticos. Os métodos de busca de resíduos quadráticos seguintes dependem sobretudo dos conceitos de PERÍODO, GÉNERO, NÚMERO CARACTERÍSTICO, CLASSE e COMPOSIÇÃO DE FORMAS.

3.1 Primeiras definições

No artigo 153 da secção V de DA, Gauss define o objeto de estudo como as funções quadráticas em duas indeterminadas x, y da forma

$$F(x, y) = ax^2 + 2bxy + cy^2,$$

tomando $a, c \in \mathbb{Z} \setminus \{0\}$ e $b \in \mathbb{Z}$. A tal objeto chamaremos FORMAS QUADRÁTICAS BINÁRIAS podendo ser abreviado por FORMAS QUADRÁTICAS ou somente FORMAS. O coeficiente a é o COEFICIENTE INICIAL, o coeficiente b é o COEFICIENTE MÉDIO, o coeficiente c é o COEFICIENTE TERMINAL. Os coeficientes a e c também são chamados COEFICIENTES EXTREMOS. Será útil considerar a sua representação matricial mais adiante, pelo que definimos:

$$F(x, y) := \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{x}^T A \mathbf{x}. \tag{3.1}$$

Adiante, também será necessário usar ternos para nos referirmos a uma forma de maneira mais sucinta, pelo que identificamos a forma F com o terno (a, b, c).

Exemplo 3.1
A forma $F(x, y) = 3x^2 + 14xy - 8y^2$ *pode ser representada como o terno* $(3, 7, -8)$ *ou usando matrizes*

$$F(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 7 & -8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

As próximas noções constam do artigo seguinte da obra estudada, o artigo 154.

Definição 3.2 (Representação)
Um número N inteiro representa-se por uma forma F, caso existam $m, n \in \mathbb{Z}$ t.q. $F(m,n) = N$.

Definição 3.3 (Determinante)
Seja F uma forma quadrática binária (a,b,c). O DETERMINANTE é o número $b^2 - ac$. Denotá-lo-emos por D ou $\det(F)$.

Observação 3.4 (Observação matricial)
Com uma simples conta, notamos que esta noção de determinante assemelha-se à noção moderna de determinante, já que

$$D = -\det\begin{pmatrix} a & b \\ b & c \end{pmatrix} = -\det(A).$$

Observação 3.5 (Determinantes e formas quadráticas binárias)
Seja $F(x,y) = ax^2 + 2bxy + cy^2$ uma forma quadrática binária. Podemos relacioná-la com o seu determinante da seguinte forma:

$$\begin{aligned} F(x,y) = ax^2 + 2bxy + cy^2 &\iff af(x,y) = a(ax^2 + 2bxy + cy^2) = (ax)^2 + 2abxy + acy^2 \\ &\iff af(x,y) = (ax)^2 + 2abxy + (by)^2 - (by)^2 + acy^2 \\ &\iff af(x,y) = (ax + by)^2 - (b^2 - ac)y^2 = (ax + by)^2 - Dy^2. \end{aligned}$$

Analogamente, temos também:

$$F(x,y) = ax^2 + 2bxy + cy^2 \iff cf(x,y) = (bx + cy)^2 - (b^2 - ac)x^2 = (bx + cy)^2 - Dx^2.$$

Teorema 3.6 (Artigo 154, DA)
Seja $F(x,y) = ax^2 + 2bxy + cy^2$ uma forma quadrática binária. Se N se representa por F, com $f(m,n) = N$ e $\text{mdc}(m,n) = 1$, então $b^2 - ac$ é resíduo quadrático de N.

A seguinte demonstração é a demonstração original de Gauss, a qual comentaremos ligeiramente de modo a expor a ideia completamente.

Demonstração. Sejam $F(x,y) = ax^2 + 2bxy + cy^2$ e $F^*(x,y) = ax^2 - 2bxy + cy^2$. Suponhamos $N = f(m,n)$ t.q. $\text{mdc}(m,n) = 1$. Pela identidade de Bézout, consideremos μ e $\nu \in \mathbb{Z}$ t.q $m\mu + n\nu = 1$. Para simplificar notação, definimos também $P = f^*(\nu,\mu) = a\nu^2 - 2b\mu\nu + c\mu^2$. Fazemos o seguinte produto

$$NP = (am^2 + 2bmn + cn^2) \cdot (a\nu^2 - 2b\mu\nu + c\mu^2).$$

Gauss afirma que esta expressão é igual a

$$NP = \big(\mu(mb + nc) - \nu(ma + nb)\big)^2 - (b^2 - ac) \cdot \big(m\mu + n\nu\big)^2. \tag{3.2}$$

Por ser multiplo de N, sabemos que

$$NP = (am^2 + 2bmn + cn^2) \cdot (a\nu^2 - 2b\mu\nu + c\mu^2) \equiv 0 \pmod{N}.$$

Donde concluímos que

$$NP = (\mu(mb + nc) - \nu(ma + nb))^2 - (b^2 - ac) \cdot (m\mu + n\nu)^2 \equiv 0 \pmod{N}.$$

E assim, como $m\mu + n\nu = 1$

$$(\mu(mb + nc) - \nu(ma + nb))^2 \equiv (b^2 - ac) \pmod{N}. \tag{3.3}$$

Logo, $D = b^2 - ac$ é resíduo quadrático mod N.

Q.E.D.

Observação 3.7
Gauss pouco mais acrescenta a esta demonstração e não fornece qualquer intuição sobre este cálculo. No entanto, podemos usar a observação 3.5 e o lema 1.46, para ajudar à sua compreensão. Reutilizando a notação do teorema anterior, fazendo uso da observação 3.5, sabemos:

$$aN = (am + bn)^2 - (b^2 - ac)n^2 \qquad \text{e} \qquad aP = (a\nu - b\mu)^2 - (b^2 - ac)\mu^2.$$

Relembremos a primeira identidade de Brahmagupta, no lema 1.46

$$(\alpha^2 - \varepsilon\beta^2)(\gamma^2 - \varepsilon\delta^2) = (\alpha\gamma + \varepsilon\beta\delta)^2 - \varepsilon(\alpha\delta + \beta\gamma)^2. \tag{3.4}$$

Nesta identidade podemos efetuar as seguintes substituições:

$$\alpha = am + bn, \qquad \beta = n, \qquad \gamma = a\nu - b\mu, \qquad \delta = \mu, \qquad \varepsilon = b^2 - ac.$$

Deste modo, o produto no lado esquerdo da equação (3.4) coincidirá com o produto $aN \cdot aP$, o qual é também a^2NP. Desenvolvemos a primeira parcela do lado direito:

$$\begin{aligned}(\alpha\gamma + \varepsilon\beta\delta) &= (am + bn) \cdot (a\nu - b\mu) + (b^2 - ac)n\mu \\ &= (a^2m\nu - abm\mu + abn\nu - b^2n\mu + b^2n\mu - acn\mu) \\ &= (a^2m\nu - abm\mu + abn\nu - acn\mu) = a(\nu(am + bn) - \mu(bm + cn)).\end{aligned}$$

Ou seja, $(\alpha\gamma + \varepsilon\beta\delta)^2 = a^2(\nu(am + bn) - \mu(bm + cn))^2 = a^2(\mu(bm + cn) - \nu(am + bn))^2$.
Desenvolvemos a segunda parcela:

$$(\alpha\delta + \beta\gamma) = ((am + bn)\mu + n(a\nu - b\mu)) = (am\mu + bn\mu + an\nu - bn\mu) = a(m\mu + n\nu).$$

Ou seja, $(\alpha\delta + \beta\gamma)^2 = a^2(m\mu + n\nu)^2$. Podemos conjugar estes cálculos e concluir que:

$$\begin{aligned} & a^2NP = a^2(\mu(bm + cn) - \nu(am + bn))^2 - a^2(b^2 - ac)(m\mu + n\nu)^2 \\ \iff \quad & NP = (\mu(bm + cn) - \nu(am + bn))^2 - (b^2 - ac)(m\mu + n\nu)^2.\end{aligned}$$

Este último produto coincide com a simplificação da equação (3.2), tendo assim explicitado os cálculos de Gauss.

Observação 3.8
As decomposições do capítulo anterior, ax^2+cy^2, podem ser obtidas a partir da forma quadrática binária $F(x,y) = ax^2 + 0 \cdot 2xy + cy^2$, a qual tem determinante $D = 0^2 - a \cdot c = -ac$. Pelo teorema anterior, $-ac$ é resíduo quadrático módulo N. Assumindo que $\text{mdc}(x,N) = \text{mdc}(y,N) = 1$ e $F(x,y) = N$, chegámos à mesma conclusão que a proposição 2.4, após usar o lema 2.1.

Definição 3.9 (Implicação)
Sejam $F(x,y) = ax^2 + 2bxy + cy^2$ e $G(\dot{x},\dot{y}) = \dot{a}\dot{x}^2 + 2\dot{b}\dot{x}\dot{y} + \dot{c}\dot{y}^2$ formas quadráticas binárias e $\alpha,\beta,\gamma,\delta \in \mathbb{Z}$. Caso $(x,y) = (\alpha\dot{x} + \beta\dot{y}, \gamma\dot{x} + \delta\dot{y})$ dizemos que a forma F IMPLICA a forma G ou que G está CONTIDA em F.

Observação 3.10 (Representação e Implicação)
Podemos observar desde já que, caso um número N se represente pela forma G e a forma F implica a forma G, então N representa-se pela forma F.

Para os seguintes resultados, é necessário ter presente a representação matricial de uma forma quadrática F. Apresentaremos parte dos próximos resultados usando álgebra linear por comodismo de cálculo, sem nunca esquecer a representação sucinta em ternos.

Observação 3.11 (Implicação Matricial)
Sejam $F(x,y) = \mathbf{x}^T A\mathbf{x}$ e $G(\dot{x},\dot{y}) = \dot{\mathbf{x}}^T B\dot{\mathbf{x}}$ formas quadráticas binárias. Sejam $\mathbf{x}$ e $\dot{\mathbf{x}}$ os vetores coluna $(x,y)^T$ e $(\dot{x},\dot{y})^T$ respetivamente. Consideremos agora

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

a MATRIZ DE MUDANÇA DE COORDENADAS. Caso $\mathbf{x} = M\dot{\mathbf{x}}$, ou seja,

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix},$$

dizemos que a forma F IMPLICA a forma G ou que G está CONTIDA em F. Podemos notar $F \to G$. Isto significa que $G(x,y) = \dot{\mathbf{x}}^T M^T A M \dot{\mathbf{x}}$ e que $B = M^T A M$.

É importante realçar a seguinte propriedade sobre a implicação de formas quadráticas, agora que podemos fazer uso da sua formalização matricial.

Proposição 3.12 (Transitividade)
Se a forma F implica a forma G e a forma G implica a forma H, então F implica a forma H.

Demonstração. Sejam $F(x,y) = \mathbf{x}^T A\mathbf{x}$, $G(\dot{x},\dot{y}) = \dot{\mathbf{x}}^T B\dot{\mathbf{x}}$ e $H(\ddot{x},\ddot{y}) = \ddot{\mathbf{x}}^T C\ddot{\mathbf{x}}$ formas. Por hipótese, temos que

$$G(x,y) = \dot{\mathbf{x}}^T M_0^T A M_0 \dot{\mathbf{x}} \qquad \text{e} \qquad H(x,y) = \ddot{\mathbf{x}}^T M_1^T B M_1 \ddot{\mathbf{x}}.$$

Donde concluímos que $C = M_1^T B M_1 = M_1^T M_0^T A M_0 M_1 = (M_0 M_1)^T A (M_0 M_1)$.
Logo, F implica H.

Q.E.D.

Supondo que $F \to G$, pelas propriedades da função determinante, sabemos que

$$\det(B) = \det(M^T) \cdot \det(A) \cdot \det(M).$$

Deste modo,

$$\dot{b}^2 - \dot{a}\dot{c} = (b^2 - ac) \cdot (\alpha\delta - \beta\gamma)^2. \tag{3.5}$$

Da equação 3.5, retiramos que o determinante de G é múltiplo do determinante de F e que terão o mesmo sinal já que o seu quociente é um quadrado.

Definição 3.13 (Transformações próprias e impróprias)
Consideremos a transformação $(x, y) = (\alpha\dot{x}+\beta\dot{y}, \gamma\dot{x}+\delta\dot{y})$. Dizemos que é uma TRANSFORMAÇÃO PRÓPRIA caso $(\alpha\delta - \beta\gamma) > 0$ e é uma TRANSFORMAÇÃO IMPRÓPRIA caso $(\alpha\delta - \beta\gamma) < 0$.

Definição 3.14 (Equivalência)
Caso F implique G e G implique F, dizemos que F e G são EQUIVALENTES, e denotamos $F \leftrightarrow G$.

Observação 3.15
Caso F e G sejam equivalentes, se o número N se pode representar por uma das formas, também se poderá representar pela outra.

Proposição 3.16
Caso $F = (a, b, c)$ e $G = (\dot{a}, \dot{b}, \dot{c})$ sejam equivalentes, então $\dot{b}^2 - \dot{a}\dot{c} = b^2 - ac$ e $(\alpha\delta - \beta\gamma)^2 = 1$.

Demonstração. Os determinantes dividem-se mutuamente e, como têm o mesmo sinal, têm de ser iguais.

Q.E.D.

Podemos aglomerar as últimas definições e observações para a próxima definição.

Definição 3.17
Sejam F e G formas quadráticas binárias.

- IMPLICAÇÃO PRÓPRIA: Caso F implique G por via de uma transformação própria. Neste caso, dizemos que F IMPLICA PROPRIAMENTE G ou que G está CONTIDA PROPRIAMENTE em F.
- EQUIVALÊNCIA PRÓPRIA: Caso F implique propriamente G e G implique propriamente F, dizemos que F e G são PROPRIAMENTE EQUIVALENTES, e denotamos $F \leftrightarrow_p G$.

Mutatis mutandis, podemos definir IMPLICAÇÃO IMPRÓPRIA e EQUIVALÊNCIA IMPRÓPRIA.

Podemos simplificar a noção de equivalência de formas quadráticas considerando explicitamente a sua representação matricial.

Observação 3.18 (Equivalência Matricial)
Sejam $F(x, y) = \mathbf{x}^T A\mathbf{x}$ e $G(\dot{x}, \dot{y}) = \dot{\mathbf{x}}^T B\dot{\mathbf{x}}$ formas quadráticas binárias. Suponhamos que $F \to G$ e seja M a matriz de mudança de coordenadas tal que $\mathbf{x} = M\dot{\mathbf{x}}$ e $\det^2(M) = 1$. Neste caso, F e G são equivalentes.

Observação 3.19
Tendo F e G duas formas quadráticas binárias equivalentes, então a equivalência será própria se $\det(M) = (\alpha\delta - \beta\gamma) = 1$ e a equivalência será imprópria se $\det(M) = (\alpha\delta - \beta\gamma) = -1$.

Exemplo 3.20
Seja $F(x,y) = 3x^2 + 14xy - 8y^2$ uma forma quadrática binária e consideremos a mudança de coordenadas $x = \dot{x} + 2\dot{y}$ e $y = 3\dot{x} + 7\dot{y}$. Matricialmente, podemos calcular:

$$G(\dot{x},\dot{y}) = \begin{pmatrix}\dot{x} & \dot{y}\end{pmatrix}\begin{pmatrix}1 & 3\\ 2 & 7\end{pmatrix}\begin{pmatrix}3 & 7\\ 7 & -8\end{pmatrix}\begin{pmatrix}1 & 2\\ 3 & 7\end{pmatrix}\begin{pmatrix}\dot{x}\\ \dot{y}\end{pmatrix} = \begin{pmatrix}\dot{x} & \dot{y}\end{pmatrix}\begin{pmatrix}-27 & -71\\ -71 & -184\end{pmatrix}\begin{pmatrix}\dot{x}\\ \dot{y}\end{pmatrix}.$$

Conclui-se que F implica $G(x,y) = -27x^2 - 142xy - 184y^2$. Como $1\cdot 7 - 3\cdot 2 = 1$, esta transformação é própria. Do mesmo modo, podemos considerar a transformação $\dot{x} = 7\dot{x} - 2\dot{y}$ e $\dot{y} = -3\dot{x} + \dot{y}$ e fazer o cálculo:

$$F(x,y) = \begin{pmatrix}x & y\end{pmatrix}\begin{pmatrix}7 & -3\\ -2 & 1\end{pmatrix}\begin{pmatrix}-27 & -71\\ -71 & -184\end{pmatrix}\begin{pmatrix}7 & -2\\ -3 & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} = \begin{pmatrix}x & y\end{pmatrix}\begin{pmatrix}3 & 7\\ 7 & -8\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}.$$

Como $7\cdot 1 - (-2)\cdot(-3) = 1$, temos uma transformação própria. Assim se prova que F e G são propriamente equivalentes.

Observação 3.21 (Artigo 159, DA)
A forma $F = (a,b,c)$ é propriamente equivalente às formas $F = (a,b,c)$ e $\dot{F} = (c,-b,a)$, mas é impropriamente equivalente às formas $\ddot{F} = (a,-b,c)$ e $\dddot{F} = (c,b,a)$, já que:

$$F(x,y) = \begin{pmatrix}x & y\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ b & c\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}, \qquad \dot{F}(\dot{x},\dot{y}) = \begin{pmatrix}\dot{x} & \dot{y}\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}a & b\\ b & c\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\dot{x}\\ \dot{y}\end{pmatrix},$$

$$\ddot{F}(\ddot{x},\ddot{y}) = \begin{pmatrix}\ddot{x} & \ddot{y}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}a & b\\ b & c\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\ddot{x}\\ \ddot{y}\end{pmatrix}, \qquad \dddot{F}(\dddot{x},\dddot{y}) = \begin{pmatrix}\dddot{x} & \dddot{y}\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}a & b\\ b & c\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\dddot{x}\\ \dddot{y}\end{pmatrix}.$$

Definição 3.22 (Formas opostas)
As formas $F = (a,b,c)$ e $\ddot{F} = (a,-b,c)$ são chamadas FORMAS OPOSTAS.

Observação 3.23
Podemos provar que há formas que são impropriamente equivalentes a elas mesmas. A forma $F = (2,3,5)$ é propriamente equivalente a $G = (1,0,1)$. Pelas transformações acima indicadas, sabemos que G é impropriamente equivalente a ela mesma, portanto, F também o será.

Definição 3.24 (Formas contíguas)
Sejam $F = (a,b,c)$, $\dot{F} = (\dot{a},\dot{b},\dot{c})$ e $\ddot{F} = (\ddot{a},\ddot{b},\ddot{c})$ formas quadráticas binárias de determinante D. Caso tenhamos $c = \dot{a}$ e $-b \equiv \dot{b} \pmod{\dot{a}}$, dizemos que F e $\dot{F}$ são FORMAS CONTÍGUAS ou FORMAS VIZINHAS. Caso seja $\ddot{c} = a$ e $-b \equiv \ddot{b} \pmod{\ddot{a}}$, então F e $\ddot{F}$ também são FORMAS CONTÍGUAS. Quando o contexto não for claro, diremos que a forma $\dot{F}$ é contígua à parte terminal de F e $\ddot{F}$ é contigua à parte inicial de F.

Exemplo 3.25
Sejam $F = (3, 7, -8)$ *e* $G = (-8, 1, 9)$. *Temos que* $\det(F) = \det(G) = 73$ *e como* $7 \equiv -1 \pmod{-8}$ *e* $-8 = c = \dot{a}$, F *e* G *são formas contíguas.*

Observação 3.26
Se F e G são duas formas contíguas, então F e G são propriamente equivalentes. Isto pode ver-se, dado que F implicará uma forma contígua fazendo uma mudança de coordenadas,

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & \frac{b+\dot{b}}{c} \end{pmatrix} \begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix}.$$

Definição 3.27 (Forma ambígua)
Uma forma quadrática binária $F = (a, b, c)$ tal que $a \mid 2b$ chama-se FORMA AMBÍGUA.

Suponhamos que F é uma forma quadrática ambígua. A forma $G = (c, b, a)$ é contígua à primeira parte de F, logo é propriamente equivalente a F. Pelos cálculos matriciais anteriores, sabemos que G é impropriamente equivalente a F. Logo F é tanto propriamente como impropriamente equivalente a G. Como F é propriamente equivalente a si mesma, (observação 3.21), F também será impropriamente equivalente a si mesma, justificando a denominação de forma ambígua.

3.2 Determinante de formas quadráticas binárias

Gauss analisou o comportamento distinto de formas quadráticas binárias com respeito à natureza do seu determinante. Analisaremos os casos quando o determinante das mesmas é negativo e quando o determinante é positivo sem ser um quadrado perfeito. Omitimos o caso em que o determinante é um quadrado perfeito, pois não será útil para os métodos de fatorização de Gauss. Antes de mais nada, é importante definir um conceito importante.

Definição 3.28 (Congruente mínimo absoluto)
Seja $b \in \mathbb{Z}$ e $a \in \mathbb{Z} \setminus \{0\}$ e definamos $\mathrm{Cong}(b, a) = \{x \in \mathbb{Z} \mid x \equiv b \pmod{a}\}$ como o conjunto dos números congruentes a b módulo a. Ao elemento de $\mathrm{Cong}(b, a)$ com o menor valor absoluto chamamos CONGRUENTE MÍNIMO ABSOLUTO DE b MÓDULO a.

Exemplo 3.29
Sejam $b = 5$, $a = 7$. *Podemos calcular* $\mathrm{Cong}(5, 7) = \{\ldots, -9, -2, 5, 12, \ldots\}$ *e como* $|-2| < |5| < |-9| < |12|$, *vem que* -2 *é o congruente mínimo absoluto de* 5 *módulo* 7.

Observação 3.30 (Nota prévia)
Os trabalhos de Gauss não usam módulos, o que complica a sua leitura. Nesta secção, querendo ser fiel à obra original, adaptámos alguns resultados e demonstrações para refletir esta alteração.

3.2.1 Determinante negativo

Definição 3.31 (Forma reduzida)
Seja $F = (a, b, c)$ uma forma quadrática binária de determinante $D < 0$. Caso $|2b| \leqslant |a| \leqslant |c|$ e $|a| \leqslant \sqrt{\frac{4|D|}{3}}$, dizemos que F é uma FORMA QUADRÁTICA BINÁRIA REDUZIDA. Podemos abreviar esta denominação por FORMA QUADRÁTICA REDUZIDA ou só FORMA REDUZIDA.

Teorema 3.32
Seja $F = (a, b, c)$ t.q. $D < 0$. Então, existe uma forma $G = (A, B, C)$ propriamente equivalente a F t.q. G é uma forma reduzida.

A demonstração é construtiva, e usa um algoritmo que enunciamos abaixo. No final, demonstramos que a forma final que se obtém tem de ser reduzida.

Algoritmo de redução para formas de determinante negativo
Seja F uma forma quadrática binária com determinante $D < 0$. 1. Caso F seja reduzida, o algoritmo termina aqui, e $F = G$. 2. Passo-base: $F = F_0 = (a_0, b_0, a_1)$ e $i = 0$. 3. Tomemos b_{i+1} como o congruente mínimo absoluto de $-b_i$ módulo a_{i+1} e $a_{i+2} = \frac{b_{i+1}^2 - D}{a_{i+1}}$. - Esta fração é um número inteiro, pois temos que $a_i a_{i+1} = b_i^2 - D$, donde $$b_{i+1}^2 \equiv b_i^2 \pmod{a_{i+1}} \iff b_{i+1}^2 - D \equiv b_i^2 - D \equiv 0 \pmod{a_{i+1}}.$$ - Pela definição de congruente mínimo absoluto, $\lvert b_{i+1}\rvert \leqslant \frac{1}{2}\cdot\lvert a_{i+1}\rvert$. Logo, $\lvert 2b_{i+1}\rvert \leqslant \lvert a_{i+1}\rvert$. 4. Obtemos a forma $F_{i+1} = (a_{i+1}, b_{i+1}, a_{i+2})$. 5. Caso $\lvert a_{i+2}\rvert < \lvert a_{i+1}\rvert$, voltamos ao passo 3 e $i \longrightarrow i + 1$.
No final, temos uma forma $F_m = (a_m, b_m, a_{m+1})$ tal que $\lvert a_m\rvert \leqslant \lvert a_{m+1}\rvert$ e pomos $F_m := G$.

Tabela 3.1: Algoritmo de redução para formas quadráticas binárias com determinante negativo

Demonstração. Veremos adiante que a forma final deste algoritmo será reduzida.

1. Sabemos que o algoritmo chega a um final, pois caso contrário teriamos uma sequência decrescente de números naturais infinita, o que é absurdo.

2. Na progressão de formas $F_0, F_1, F_2, \ldots, F_m$ cada forma é contígua à anterior. Pelas observações 3.19 e 3.26, $F_0 = (a_0, b_0, a_1)$ e $F_m = (a_m, b_m, a_{m+1})$ são propriamente equivalentes.

3. Sabemos que b_m é o menor representante positivo de $-b_{m-1}$ módulo a_m, pelo que se tem $\lvert b_m\rvert \leqslant \frac{1}{2}\cdot\lvert a_m\rvert \Longrightarrow 2\lvert b_m\rvert \leqslant \lvert a_m\rvert$. Como $2\lvert b_m\rvert \geqslant \lvert 2b_m\rvert$, segue que $\lvert 2b_m\rvert \leqslant \lvert a_m\rvert$.

4. Suponhamos que temos $F_m = (a_m, b_m, a_{m+1})$ tal que $\lvert a_m\rvert \leqslant \lvert a_{m+1}\rvert$. Deste modo, sabemos que $\lvert a_m\rvert^2 \leqslant \lvert a_m a_{m+1}\rvert$. Da equação $D = b_m^2 - a_m a_{m+1}$ segue que $\lvert D - b_m^2\rvert = \lvert a_m a_{m+1}\rvert$. Portanto, $\lvert a_m\rvert^2 \leqslant \lvert D - b_m^2\rvert$. Pela desigualdade triangular e pelo item anterior,

$$\lvert a_m\rvert^2 \leqslant \lvert D - b_m^2\rvert \leqslant \lvert D\rvert + \lvert b_m^2\rvert \leqslant \lvert D\rvert + \frac{1}{4}\lvert a_m\rvert^2.$$

Em conclusão, $\frac{3}{4}\lvert a_m\rvert^2 \leqslant \lvert D\rvert$. Logo, $\lvert a_m\rvert \leqslant \sqrt{\frac{4\lvert D\rvert}{3}}$.

Q.E.D.

Exemplo 3.33
Queremos determinar uma forma reduzida propriamente equivalente à forma $F = (304, 217, 155)$. *O determinante da forma é* $D = 217^2 - 304 \cdot 155 = -31$.

- $F_0 = (a_0, b_0, a_1) = (304, 217, 155)$
  - *Como* $-217 \equiv -62 \pmod{155}$, *logo* $b_1 = -62$. *Donde,* $a_2 = \frac{b_1^2 - D}{a_1} = \frac{(-62)^2+31}{155} = 25$. *Assim,* $F_1 = (a_1, b_1, a_2) = (155, -62, 25)$. *No final,* $a_2 = |25| < |155| = a_1$, *a forma não é reduzida.*
- $F_1 = (a_1, b_1, a_2) = (155, -62, 25)$
  - *Como* $62 \equiv 12 \pmod{25}$, *logo* $b_2 = 12$. *Donde,* $a_3 = \frac{b_2^2 - D}{a_2} = \frac{12^2+31}{25} = 7$. *Assim,* $F_2 = (a_2, b_2, a_3) = (25, 12, 7)$. *No final,* $a_3 = |7| < |25| = a_2$, *a forma não é reduzida.*
- $F_2 = (a_2, b_2, a_3) = (25, 12, 7)$
  - *Como* $-12 \equiv 2 \pmod{7}$, *logo* $b_3 = 2$. *Donde,* $a_4 = \frac{b_3^2 - D}{a_3} = \frac{2^2+31}{7} = 5$. *Assim,* $F_3 = (a_3, b_3, a_4) = (7, 2, 5)$. *No final,* $a_4 = |5| < |7| = a_3$, *a forma não é reduzida.*
- $F_3 = (a_3, b_3, a_4) = (7, 2, 5)$
  - *Como* $-2 \equiv -2 \pmod{5}$, *logo* $b_3 = 2$. *Donde,* $a_5 = \frac{b_4^2 - D}{a_4} = \frac{(-2)^2+31}{5} = 7$. *Assim,* $F_4 = (a_4, b_4, a_5) = (5, -2, 7)$. *No final,* $a_4 = |5| < |7| = a_5$, *a forma é reduzida.*

Logo, a forma reduzida propriamente equivalente a F *é* $(5, -2, 7)$.

Após enunciar e demonstrar este algoritmo de redução de formas quadráticas, nos artigos 172 e 173 do DA, Gauss procura estabelecer os critérios para a equivalência própria e imprópria de duas formas quadráticas reduzidas com o mesmo determinante negativo D.

Teorema 3.34 (Artigo 173, DA)
Sejam F, G duas formas quadráticas de determinante negativo e tomemos f e g duas formas quadráticas reduzidas que lhes são propriamente equivalentes, respetivamente. Então, vem que:

1. As formas F e G não são equivalentes, se f e g não são idênticas nem opostas.
2. As formas F e G são apenas propriamente equivalentes, se f e g são idênticas sem ser ambiguas ou ter os coeficientes extremos iguais.
3. As formas F e G são impropriamente equivalentes, se f e g são opostas, mas não são nem ambiguas nem têm os coeficientes extremos iguais.
4. As formas F e G são propriamente e impropriamente equivalentes se f e g são, em primeiro lugar, idênticas ou opostas e, em segundo lugar, ou ambiguas ou têm os coeficientes extremos iguais.

A demonstração deste teorema é bastante técnica, pelo que a omitimos, mas esta pode ser encontrada no artigo 172 do DA.

Técnicas para encontrar todas as formas reduzidas de determinante D

Queremos encontrar todas as formas quadráticas binárias (a, b, c) que sejam reduzidas e tenham determinante $D = b^2 - ac$.

Primeira técnica

Para o coeficiente inicial, consideremos todos os números inteiros a tais que $|a| \leqslant \sqrt{\frac{4|D|}{3}}$, para os quais a congruência $x^2 \equiv D \pmod{a}$ é possível, pela definição de determinante. Para cada um desses valores, tomamos b o valor positivo da expressão $\sqrt{D}$ módulo a inferior ou igual a $\frac{a}{2}$. Para cada b encontrado, também consideramos o valor $-b$ como possível coeficiente. De forma a calcular o último coeficiente, calculemos $c = \frac{b^2-D}{a}$. Se nestes calculos, obtivermos formas nas quais $c < a$, basta descartar essas formas.

Exemplo 3.35

Procuramos todas as formas reduzidas com determinante $D = -85$. Como devem ser reduzidas, vem que $|a| \leqslant \sqrt{\frac{4\cdot|-85|}{3}} < 11$. Para os valores positivos de a, consideramos os números entre 1 e 10 tais que a congruência $x^2 \equiv -85 \pmod{a}$ é possível. Estes números são 1, 2, 5 e 10.

- $F_0 = (1, 0, 85)$
  - *Escolhemos $a = 1$, donde $b = \sqrt{-85} \pmod 1 = 0$, e portanto $c = \frac{0^2+85}{1} = 85$.*
- $F_1 = (2, 1, 43), F_2 = (2, -1, 43)$
  - *Escolhemos $a = 2$, donde $b = \sqrt{-85} \pmod 2 = \pm 1$, e portanto $c = \frac{(\pm1)^2+85}{2} = 43$.*
- $F_3 = (5, 0, 17)$
  - *Escolhemos $a = 5$. Como $5 \mid D$, vem que $\sqrt{-85} \pmod 5 = 0$, logo $c = \frac{0^2+85}{5} = 17$.*
- $F_4 = (10, 5, 11)$, $F_5 = (10, -5, 11)$
  - *Escolhemos $a = 10$. Segue que $b = \sqrt{-85} \pmod{10} = \pm 5$, e portanto $c = \frac{(\pm5)^2+85}{10}$.*

Do mesmo modo, podemos considerar os valores negativos de a e fazendo cálculos semelhantes, obtemos as formas $F_6 = (-1, 0, -85)$, $F_7 = (-2, 1, -43)$, $F_8 = (-2, -1, -43)$, $F_9 = (-5, 0, -17)$, $F_{10} = (-10, 5, -11)$, $F_{11} = (-10, -5, -11)$.

Segunda técnica

Para o coeficiente médio b, consideramos todos os números inteiros cujo valor absoluto seja inferior ou igual a $\sqrt{\frac{|D|}{3}}$. Para cada b, fatorizamos $b^2 - D$ de todas as formas possíveis em pares de fatores nas quais nenhum dos elementos é inferior a $2b$ em valor absoluto. Quando os valores são diferentes, tomamos a como o menor valor e c o maior valor. Por construção, $a \leqslant \sqrt{\frac{4|D|}{3}}$.

Os métodos estudados encontram todas as formas reduzidas, no entanto, algumas das formas encontradas serão propriamente equivalentes entre si, pelo que podemos descartá-las. Usando o teorema 3.34, para o determinante -85 sobram somente as 8 formas:

$$(1, 0, 85),\ (2, 1, 43),\ (5, 0, 17),\ (10, 5, 11),\ (-1, 0, -85),\ (-2, 1, -43),\ (-5, 0, -17),\ (-10, 5, -11).$$

3.2.2 Determinante positivo não-quadrado

Definição 3.36 (Forma reduzida)
Seja $F = (a, b, c)$ uma forma quadrática de determinante D positivo e não-quadrado. Caso seja $\sqrt{D} - b \leqslant |a| \leqslant \sqrt{D} + b$ e que $0 < b < \sqrt{D}$, então F é uma FORMA QUADRÁTICA BINÁRIA REDUZIDA. Podemos abreviar esta denominação por FORMA QUADRÁTICA REDUZIDA, ou só FORMA REDUZIDA.

Observação 3.37
Da definição anterior, deduzimos o enquadramento $\sqrt{D} > b \geqslant \sqrt{D} - |a|$.

Teorema 3.38
Seja $F = (a, b, c)$ uma forma quadrática binária de determinante D positivo e não-quadrado. Então, existe uma forma quadrática reduzida $G = (A, B, C)$ propriamente equivalente a F.

Algoritmo de redução para formas de determinante positivo e não-quadrado.
Seja F uma forma quadrática binária de determinante não-quadrado $D > 0$.
1. Caso F seja reduzida, o algoritmo termina aqui, e $F = G$
2. Passo-base: $F = F_0 = (a_0, b_0, a_1)$ e $i = 0$
3. Tomemos $b_{i+1} \equiv -b_i \pmod{a_{i+1}}$ tal que $\sqrt{D} - \lvert a_{i+1}\rvert \leqslant b_{i+1} < \sqrt{D}$ e $a_{i+2} = \frac{b_{i+1}^2 - D}{a_{i+1}}$.
- Esta fração é um número inteiro, pois temos que $a_i a_{i+1} = b_i^2 - D$, donde $b_{i+1}^2 \equiv b_i^2 \pmod{a_{i+1}} \iff b_{i+1}^2 - D \equiv b_i^2 - D \equiv 0 \pmod{a_{i+1}}$
4. Obtemos a forma $F_{i+1} = (a_{i+1}, b_{i+1}, a_{i+2})$.
5. Caso $\lvert a_{i+2}\rvert < \lvert a_{i+1}\rvert$, voltamos ao passo 3 e $i \longrightarrow i + 1$.
No final, temos uma forma $F_m = (a_m, b_m, a_{m+1})$ tal que $\lvert a_m\rvert \leqslant \lvert a_{m+1}\rvert$ e pomos $F_m := G$.

Tabela 3.2: Algoritmo de redução para formas quadráticas binárias de determinante positivo e não-quadrado

Lema 3.39
Os coeficientes a_m e a_{m+1} têm sinais opostos.

Demonstração. Suponhamos que $a_m a_{m+1} > 0$. Isto significa que $b_m^2 - D > 0$. Logo $b_m^2 > D$. Pelo algoritmo, vem que $\sqrt{D} > b_m$, logo $D > b_m\sqrt{D}$. Donde $b_m^2 > D > b_m\sqrt{D}$, pelo que

$$b_m^2 - b_m\sqrt{D} = b_m(b_m - \sqrt{D}) > 0. \tag{3.6}$$

Pelo algoritmo, $(b_m - \sqrt{D}) < 0$. Logo, pela desigualdade 3.6 conclui-se que $b_m < 0$.
Pelo algoritmo, sabemos que $\sqrt{D} - |a_m| \leqslant b_m$. Como $b_m < 0$, vem que $0 < \sqrt{D} < |a_m| + b_m$.
Também porque $b_m < 0$, segue que $|a_m| - b_m > 0$. Assim, $(|a_m| - b_m)(|a_m| + b_m) = a_m^2 - b_m^2 > 0$.
Ou seja, $a_m^2 > b_m^2$.

Pela condição de paragem do algoritmo, $|a_m| \leqslant |a_{m+1}|$, logo $|a_m|^2 = a_m^2 \leqslant |a_m a_{m+1}| = a_m a_{m+1}$.
Por fim, $a_m a_{m+1} \geqslant a_m^2 > b_m^2$. Ou seja, $0 > b_m^2 - a_m a_{m+1}$. Logo, $D < 0$. Absurdo.

Q.E.D.

Demonstração. Queremos demonstrar que a forma quadrática binária final obtida é reduzida:

1. Sabemos que o algoritmo chega a um final, pois caso contrário teriamos uma sequência decrescente de números naturais infinita, o que é absurdo.

2. Na progressão de formas $F_0, F_1, F_2, \ldots, F_m$ cada forma é contígua à anterior. Pelas observações 3.19 e 3.26, $F_0 = (a_0, b_0, a_1)$ e $F_m = (a_m, b_m, a_{m+1})$ são propriamente equivalentes.

3. Queremos provar que $|a_m|$ está situado entre $\sqrt{D} - b_m$ e $\sqrt{D} + b_m$.
Pelo algoritmo, $b_m \geqslant \sqrt{D} - |a_m|$, logo $|a_m| \geqslant \sqrt{D} - b_m$. Como $|a_m| \leqslant |a_{m+1}|$, vem que $|a_m|^2 \leqslant |a_m a_{m+1}| = |D - b_m^2|$. Pelo lema 3.39 vem que $a_m a_{m+1} < 0$. Deste modo, $b_m^2 - D < 0$ e assim, $D - b_m^2 > 0$. Portanto, $|D - b_m^2| = D - b_m^2 < D$. Logo, temos que $|a_m|^2 < D$ e assim $|a_m| < \sqrt{D}$. Portanto, $b_m > \sqrt{D} - |a_m| > 0$. Assim, concluimos que b_m e $\sqrt{D} - |a_m|$ são positivos. Logo, $b_m + \sqrt{D} - |a_m| > 0$, e assim, $\sqrt{D} + b_m > |a_m|$.

Q.E.D.

Observação 3.40
A condição de paragem do algoritmo anterior é $|a_m| \leqslant |a_{m+1}|$. O ponto 3 da demonstração do algoritmo mostra que é uma condição suficiente para termos uma forma reduzida, mas não é necessária. No exemplo 3.45, a forma $(-9, 4, 7)$ que não cumpre esta condição e é reduzida.

Exemplo 3.41
Queremos encontrar uma forma reduzida propriamente equivalente a $F = (67, 97, 140)$. *Sabemos que* $\det(F) = 97^2 - 67 \cdot 140 = 29$.

- $F_0 = (67, 97, 140)$
  - $b_1 \equiv -97 \pmod{140}$. *Como* $-134,61 \approx \sqrt{D} - 140 < b_1 < \sqrt{D} \approx 5,38$, *escolhemos* $b_1 = -97$. *Assim,* $a_2 = \frac{(-97)^2 - 29}{140} = 67$. *Como* $|a_2| < |a_1|$, *a forma não é reduzida.*
- $F_1 = (140, -97, 67)$
  - $b_2 \equiv 97 \equiv -37 \pmod{67}$. *Como* $-61,61 \approx \sqrt{D} - 67 < b_2 < \sqrt{D} \approx 5,38$, *escolhemos* $b_2 = -37$. *Assim,* $a_3 = \frac{(-37)^2 - 29}{67} = 20$. *Como* $|a_3| < |a_2|$, *a forma não é reduzida.*
- $F_2 = (67, -37, 20)$
  - $b_3 \equiv 37 \equiv -3 \pmod{20}$. *Como* $-14,61 \approx \sqrt{D} - 20 < b_3 < \sqrt{D} \approx 5,38$, *escolhemos* $b_3 = -3$. *Assim,* $a_4 = \frac{(-3)^2 - 29}{20} = -1$. *Como* $|a_4| < |a_3|$, *a forma não é reduzida.*
- $F_3 = (20, -3, -1)$
  - $b_4 \equiv 3 \equiv 5 \pmod{-1}$. *Como* $4,38 \approx \sqrt{D} - |-1| < b_4 < \sqrt{D} \approx 5,38$, *escolhemos* $b_4 = 5$. *Assim,* $a_5 = \frac{5^2 - 29}{-1} = 4$. *Como* $|a_5| > |a_4|$, *a forma é reduzida.*

Assim, a forma reduzida é $F_4 = (-1, 5, 4)$.

Após estabelecer critérios para determinar se duas formas quadráticas com determinante negativo são equivalentes, Gauss tenta resolver o mesmo problema para formas de determinante positivo não quadrado. No entanto, estas proporcionam uma análise mais subtil. O artigo 184 do DA mostra que uma forma quadrática pode ter várias formas quadráticas reduzidas que lhe são propriamente equivalentes. Tal como Gauss, começaremos por apresentar resultados menores que nos preparam para um resultado importante.

Proposição 3.42 (Artigo 184, DA)
Seja $F = (a, b, c)$ uma forma quadrática binária reduzida de determinante D positivo e não-quadrado.

1. Os coeficientes extremos a e c têm sinais opostos.
2. Os números $|a|$ e $|c|$ situam-se entre $\sqrt{D} - b$ e $\sqrt{D} + b$, pelo que a forma $\ddot{F} = (c, b, a)$ é também uma forma reduzida.
3. A partir da definição de forma reduzida, deduzimos que $|a|, |c| < 2\sqrt{D}$.
4. Por termos $\sqrt{D} - |a| < b < \sqrt{D}$, segue-se que $\sqrt{D} - |c| < b < \sqrt{D}$.

Teorema 3.43 (Artigo 184, DA)
Seja $F = (a, b, c)$ uma forma quadrática reduzida com determinante D positivo e não-quadrado. Então, só existe uma forma reduzida contígua à parte inicial de F e outra à parte terminal de F.

Demonstração. Sejam $\dot{a} = c$ e $\dot{b} \equiv -b \pmod{\dot{a}}$ tal que $\sqrt{D} - |\dot{a}| < \dot{b} < \sqrt{D}$. Suponhamos que

$$\sqrt{D} + b - |\dot{a}| = p, \qquad |\dot{a}| - (\sqrt{D} - b) = q, \qquad \sqrt{D} - b = r.$$

Pela proposição anterior e pela definição de forma reduzida, segue que $p, q, r > 0$. Suponhamos também

$$\dot{b} - (\sqrt{D} - |\dot{a}|) = \dot{q} \qquad \text{e} \qquad \sqrt{D} - \dot{b} = \dot{r}.$$

Pela definição de $\dot{b}$, vem que $\dot{q}, \dot{r} > 0$. Sabemos que $b + \dot{b} = m|\dot{a}|$ tal que $m \in \mathbb{Z}$. Por conseguinte, $b + \dot{b} = p + \dot{q} > 0$. Deste modo, $m|\dot{a}| > 0$ e assim $m > 0$, portanto $m - 1 \geqslant 0$. Em consequência,

$$r + \dot{q} + m|\dot{a}| = 2\dot{b} + |\dot{a}| \iff 2\dot{b} = r + \dot{q} + (m-1)|\dot{a}|.$$

Deste modo, $2\dot{b} > \dot{b} > 0$. Como $\dot{b} + \dot{r} = \sqrt{D}$, então $\dot{b} < \sqrt{D}$. Por se ter $r + m|\dot{a}| = \sqrt{D} + \dot{b}$, segue-se que $r + (m-1)|\dot{a}| = \sqrt{D} + \dot{b} - |\dot{a}| = p > 0$. Donde, como $\dot{q} > 0$, $\sqrt{D} + \dot{b} > |\dot{a}| > \sqrt{D} - \dot{b}$. A forma $(\dot{a}, \dot{b}, \dot{c})$ é contigua a F pela parte terminal e é reduzida. O raciocinio para formas contiguas à parte inicial de F é análogo.

Q.E.D.

Este teorema revela que, supondo que o determinante é positivo e não-quadrado, cada forma quadrática binária reduzida será contígua à parte final de outra forma quadrática binária reduzida com o mesmo determinante. Mais concretamente, seja F_0 forma reduzida de determinante D. Podemos tomar F_1 forma reduzida contígua a F_0. Então, continuando o processo, a forma reduzida F_2 será contígua a F_1, a forma reduzida F_3 será contígua a F_2, etc.

Deste modo, determinamos uma progressão de formas $(F_i)_{i\geqslant 0} = (F_0, F_1, F_2, F_3, \ldots)$ propriamente equivalentes entre si. O número de formas reduzidas para um determinante D é finito, e teremos a demonstração de tal facto no lema 3.47. Por isso, terá de haver formas repetidas a partir de um momento. Supondo que F_m e F_{m+n} são idênticas, então F_{m-1} e F_{m+n-1} também o serão e, depois de algumas iterações, F_0 e F_n. Acabamos esta subsecção com o seguinte conceito.

Definição 3.44 (Período)
Seja F_0 forma quadrática binária reduzida de determinante D positivo e não-quadrado. Chamamos Período à progressão de formas $P = (F_i)_{0\leqslant i\leqslant n-1} = (F_0, F_1, \ldots, F_{n-1})$ propriamente equivalentes enunciada no parágrafo anterior, sendo F_n idêntica a F_0.

Exemplo 3.45
A demonstração do teorema 3.43 mostra que podemos usar o algoritmo de redução enunciado no início desta subsubsecção para calcular o período da forma quadrática reduzida $F_0 = (3, 8, -5)$. Explicitemos as contas para o próximo termo do período da forma $F_0 = (3, 8, -5)$.

Seja $F_0 = (3, 8, -5)$, de determinante $D = 79$. Queremos calcular a forma F_1. Tomamos $b_1 \equiv -8 \pmod{-5}$. Como temos de ter $-3,88 \approx \sqrt{D} - 5 < b_1 < \sqrt{D} \approx 8,88$, escolhemos $b_1 = 7$. Assim, $a_2 = \frac{7^2-79}{-5} = 6$, ou seja, $F_1 = (-5, 7, 6)$. Continuando deste modo, o período é

$$(3, 8, -5),\ (-5, 7, 6),\ (6, 5, -9),\ (-9, 4, 7),\ (7, 3, -10),\ (-10, 7, 3).$$

Técnicas para encontrar todas as formas reduzidas de determinante positivo não quadrado D

Primeira técnica
Para b, tomamos todos os números positivos inferiores a $\sqrt{D}$. Para cada valor considerado, separamos $b^2 - D$ em pares de fatores de forma a que o valor absoluto de cada fator esteja entre $\sqrt{D} + b$ e $\sqrt{D} - b$. Atribuimos a a um desses fatores e a c o fator remanescente.

Segunda técnica
Para o coeficiente inicial, tomamos todos os números inteiros a t.q. $|a| < 2\sqrt{D}$ (Proposição 3.42), para os quais a congruência $x^2 \equiv D \pmod{a}$ é possível. Para cada a encontrado, tomamos para b todos os valores positivos da expressão $\sqrt{D}$ módulo a situados entre $\sqrt{D}$ e $\sqrt{D} - |a|$. Tendo estes números escolhidos, basta calcular $\frac{b^2-D}{a}$ para obter o coeficiente restante. Descartamos as formas para as quais não tenhamos $|a|$ entre $\sqrt{D} + b$ e $\sqrt{D} - b$.

Exemplo 3.46
Queremos encontrar todas as formas reduzidas com determinante 79. Só usaremos a segunda técnica. Para termos o primeiro limite para a, basta calcular $a < 2\sqrt{D} \approx 17,77$. Deste modo, escolhemos os valores a para os quais a congruência $x^2 \equiv 79 \pmod{a}$ é possível. Por facilidade de cálculo, comecemos pelos valores positivos de a. Para os valores negativos, só precisaremos de trocar os sinais dos coeficientes extremos (Proposição 3.42). Isto significa que $a = 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15$ e os valores de b são os valores positivos de $\sqrt{D}$ módulo a entre $\sqrt{D}$ e $\sqrt{D} - |a|$. O valor de c pode ser deduzido através da equação $D = b^2 - ac$. Calculemos só algumas formas, pois poderemos calcular as remanescentes seguindo o algoritmo.

- $G = (5, 7, -6)$ *e* $H = (5, 8, -3)$
  - *Seja* $a = 5$. *Para encontrar o valor de* b, *queremos resolver* $x^2 \equiv 79 \pmod 5$ *de forma a que* $3,88 \approx \sqrt{D} - a \leqslant x < \sqrt{D} \approx 8,88$. *Por tentativa e erro vem que* $x = \pm 2$. *Donde deduzimos que* $b = 7, 8$ *e* $c = -6, -3$ *respetivamente.*
- $E = (14, 3, -5)$. *Desconsiderada.*
  - *Seja* $a = 14$. *Para encontrar o valor de* b, *queremos resolver* $x^2 \equiv 79 \pmod{14}$ *de forma a que* $-4,11 \approx \sqrt{D} - a \leqslant x < \sqrt{D} \approx 8,88$. *Por tentativas, reparamos que* $x = \pm 3$, *donde vem que* $b = 3$, *pois* $b > 0$. *Assim, vem que* $c = \frac{3^2 - 79}{14} = -5$. *Isto é um problema, pois* $14 \notin [\sqrt{79} - 3, \sqrt{79} + 3]$, *pelo que temos de descartar esta forma.*

Aplicando a técnica enunciada, temos as seguintes 16 formas:

$F_0 = (1, 8, -15)$	$F_1 = (2, 7, -15)$	$F_2 = (3, 7, -10)$	$F_3 = (3, 8, -5)$
$F_4 = (5, -7, -6)$	$F_5 = (5, 8, -3)$	$F_6 = (6, 5, -9)$	$F_7 = (6, 7, -5)$
$F_8 = (7, 3, -10)$	$F_9 = (7, 4, -9)$	$F_{10} = (9, 4, -7)$	$F_{11} = (9, 5, -6)$
$F_{12} = (10, 3, -7)$	$F_{13} = (10, 7, -3)$	$F_{14} = (15, 7, -2)$	$F_{15} = (15, 8, -1)$

Tabela 3.3: As 16 formas quadráticas reduzidas binárias com coeficiente inicial positivo

Podemos calcular formas similares a estas, trocando os sinais dos coeficientes extremos:

$F_0^* = (-1, 8, 15)$	$F_1^* = (-2, 7, 15)$	$F_2^* = (-3, 7, 10)$	$F_3^* = (-3, 8, 5)$
$F_4^* = (-5, -7, 6)$	$F_5^* = (-5, 8, 3)$	$F_6^* = (-6, 5, 9)$	$F_7^* = (-6, 7, 5)$
$F_8^* = (-7, 3, 10)$	$F_9^* = (-7, 4, 9)$	$F_{10}^* = (-9, 4, 7)$	$F_{11}^* = (-9, 5, 6)$
$F_{12}^* = (-10, 3, 7)$	$F_{13}^* = (-10, 7, 3)$	$F_{14}^* = (-15, 7, 2)$	$F_{15}^* = (-15, 8, 1)$

Tabela 3.4: As 16 formas quadráticas reduzidas binárias com coeficiente inicial negativo

Temos assim 32 *formas quadráticas binárias reduzidas com determinante* 79.

Com este conceito, Gauss afirma que todas as formas reduzidas com um certo determinante D positivo e não-quadrado podem dividir-se em vários períodos. De seguida, apresentamos uma tabela contendo uma partição em períodos para as formas de determinante 79, inspirada pela visualização em ([Gau95], p.173).

Período I		(1, 8, -15)	(-15, 7, 2)	(2, 7, -15)	(-15, 8, 1)	
Período II		(-1, 8, 15)	(15, 7, -2)	(-2, 7, 15)	(15, 8, -1)	
Período III	(3, 8, -5)	(-5, 7, 6)	(6, 5, -9)	(-9, 4, 7)	(7, 3, -10)	(-10, 7, 3)
Período IV	(-3, 8, 5)	(5, 7, -6)	(-6, 5, 9)	(9, 4, -7)	(-7, 3, 10)	(10, 7, -3)
Período V	(5, 8, -3)	(-3, 7, 10)	(10, 3, -7)	(-7, 4, 9)	(9, 5, -6)	(-6, 7, 5)
Período VI	(-5, 8, 3)	(3, 7, -10)	(-10, 3, 7)	(7, 4, -9)	(-9, 5, 6)	(6, 7, -5)

Tabela 3.5: Divisão das formas quadráticas binárias reduzidas com determinante 79 por períodos

3.3 Divisão em classes

Vimos nos teoremas 3.32 e 3.38 que podemos sempre encontrar formas quadráticas binárias reduzidas as quais são equivalentes a uma forma dada.

Lema 3.47 (Formas reduzidas em número finito)
Seja $D \in \mathbb{Z}$, ou positivo e não-quadrado, ou negativo. Existe um número finito de formas reduzidas de determinante D.

Demonstração. Caso o determinante seja positivo e não-quadrado, pela definição de forma reduzida, $0 < b < \sqrt{D}$. Ou seja, há um número finito de escolhas para o coeficiente b. Como $D = b^2 - ac$, cada coeficiente b determina todos os pares (a, c) forçando a que o número de formas seja finito. Caso o determinante seja negativo, o argumento será análogo, considerando que $|a| \leqslant \sqrt{\frac{4|D|}{3}}$ e portanto o número de escolhas para b e c será finito.

Q.E.D.

Com isto em mente, no artigo 223 do DA, Gauss pretende agrupar formas quadráticas binárias tendo por base uma forma mais *simples* à qual se podem reduzir. Esta forma age como 'porta-estandarte' ou 'representante', como no conceito atual de classes de equivalência. Estas formas reduzidas facilitam o estudo das formas quadráticas binárias, pois existem em número finito.

Proposição 3.48 (Grupo modular)
Consideremos o conjunto

$$\Gamma = \left\{ M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} : m_{ij} \in \mathbb{Z},\ \det(M) = 1 \right\}.$$

O par $(\Gamma, \bullet)$ constitui um grupo, considerando $\bullet$ o produto usual de matrizes.

Proposição 3.49
A relação $\leftrightarrow_P$ da definição 3.17 e observação 3.19 é uma relação de equivalência.

Demonstração. A demonstração desta proposição é rotineira e usa sobretudo a proposição anterior, pelo que a omitimos deste texto.

Q.E.D.

Esta proposição mostra que é possível agrupar as formas quadráticas binárias em classes de equivalência para a relação $\leftrightarrow_P$. Por este motivo, é possivel selecionar uma forma quadrática de uma classe de formas como FORMA REPRESENTANTE da classe. Analisando os algoritmos de redução vistos anteriormente, vemos que estes criam uma sucessão de formas quadráticas binárias contíguas, as quais sabemos que são propriamente equivalentes, pela observação 3.26. No artigo 223 do DA, Gauss afirma que é preferível tomar a forma mais simples possível quanto à ordem de grandeza dos coeficientes, mesmo que a forma não seja reduzida, pelo que lista os critérios a considerar nesta análise:

- Caso o determinante D seja negativo, devem ser tomadas as formas reduzidas como as formas representantes, pelo teorema 3.34. No exemplo do determinante -85, as oito formas

encontradas representam as oito classes existentes. Quando há duas formas reduzidas na mesma classe, devemos tomar aquela com coeficiente médio positivo.

- Caso o determinante D seja positivo, devemos calcular o período de todas as formas reduzidas e agrupar estes períodos como visto anteriormente. Gauss demonstra no artigo 187 da obra estudada que, ou existirão duas formas ambíguas num período, ou nenhuma existirá.

  – Sejam $F_0 = (A_0, B_0, C_0)$ e $F_1 = (A_1, B_1, C_1)$ essas formas ambíguas. Para $i \in \{0, 1\}$, tomemos M_i o congruente mínimo absoluto de B_i módulo A_i tomado positivamente e $N_i = \frac{D-M_i^2}{A_i}$. Criamos as formas $F_{ri} = (A_i, M_i, -N_i)$ a partir destes elementos. Gauss considera a forma mais simples como aquela cujo coeficiente médio é 0. No caso de não ser possível, prefere-se aquela com o menor coeficiente inicial. No caso de termos duas formas com coeficientes iniciais com o mesmo valor absoluto, tomamos aquela com primeiro termo positivo. Esta será a forma representante.

  – Quando não há formas ambíguas no período, escolhemos a forma quadrática com o coeficiente inicial a de menor valor absoluto. Caso duas formas tenham termos iniciais com sinais opostos, devemos tomar aquela com o coeficiente inicial positivo. Sendo $F = (A, B, C)$ a forma escolhida, criamos a forma $F_r = (A, M, -N)$ usando o processo do item anterior (M é o congruente mínimo absoluto de B módulo A e $N = \frac{D-M^2}{A}$). Esta será a forma representante.

Exemplo 3.50
Vejamos dois exemplos do que foi visto até agora.

- *Consideremos a forma quadrática* $F_0 = (17, 4, -17)$, *com determinante* $D = 305$. *Assim, basta calcular o seu período:* $F_0 = (17, 4, -17)$, $F_1 = (-17, 13, 8)$, $F_2 = (8, 11, -23)$, $F_3 = (-23, 12, 7)$, $F_4 = (7, 16, -7)$, $F_5 = (-7, 12, 23)$, $F_6 = (23, 11, -8)$, $F_7 = (-8, 13, 17)$. *Dentro destas formas, escolhemos* F_4 *e fazendo a conta anterior, temos* $F_r = (7, 2, -43)$ *como a forma representante.*

- *Analisando a tabela do determinante* $D = 79$, *vista anteriormente, e aplicando o algoritmo enunciado, vemos que temos as 6 formas representantes:* $F_{r1} = (1, 0, -79)$, $F_{r2} = (-1, 0, 79)$, $F_{r3} = (3, 1, -26)$, $F_{r4} = (-3, 1, 26)$, $F_{r5} = (-3, -1, 26)$, $F_{r6} = (3, -1, -26)$.

3.4 Caráter de uma forma

Definição 3.51 (Primitiva)
Seja $F = (a, b, c)$ forma quadrática binária tal que $\text{mdc}(a, b, c) = 1$. Dizemos que F é PRIMITIVA.

Teorema 3.52 (Artigo 228, DA)
Seja $F = (a, b, c)$ uma forma quadrática binária primitiva e seja p um número primo dado. Existem infinitos números representados por F não divisiveis por p.

O artigo 229 da obra estudada contém considerações de extrema importância para a teoria desenvolvida por Gauss, pelo que tudo que se expõe adiante provirá de tal artigo.

Teorema 3.53 (Artigo 229, DA)
Seja $F = (a, b, c)$ uma forma quadrática primitiva com determinante D e p um número primo divisor de D. Então, todos os números representados por F ou são todos resíduos quadráticos módulo p, ou são todos não-resíduos quadráticos módulo p.

Demonstração. Suponhamos que x e x_0 são representados por F e não são múltiplos de p,

$$x = ag^2 + 2bgh + ch^2 \qquad \text{e} \qquad x_0 = ag_0^2 + 2bg_0h_0 + ch_0^2. \tag{3.7}$$

Então,

$$x \cdot x_0 = (agg_0 + b(gh_0 + g_0h) + chh_0)^2 - D(gh_0 - hg_0)^2. \tag{3.8}$$

Logo, xx_0 é resíduo quadrático módulo D. Como p divide D, xx_0 é resíduo quadrático módulo p. Logo, ou são ambos resíduos quadráticos ou são ambos não-resíduos quadráticos.

Q.E.D.

A partir da equação (3.8), Gauss estuda a relação entre o determinante de uma forma e o módulo 8, e para simplificar os cálculos também considera o módulo 4. Caso $D \equiv 1 \pmod 4$, não existe relação a ser estudada. Caso contrário, segue que:

- Módulo 4
  - Quando D é múltiplo de 4, F ou representa números inteiros da forma $4k + 1$, ou representa números inteiros da forma $4k + 3$. Tomando x e x_0 representados por F, temos que xx_0 tem de ser um resíduo quadrático módulo 4, ou seja, $xx_0 \equiv 1 \pmod 4$. Somente temos esta possibilidade se $x \equiv x_0 \equiv \pm 1 \pmod 4$.
  - Quando $D \equiv 3 \pmod 4$, F ou representa números inteiros da forma $4k + 1$, ou representa números inteiros da forma $4k + 3$. Isto vem por se poder reduzir o produto $x \cdot x_0$ a algo da forma $A^2 - DB^2$ (equação (3.8)). Quando x e x_0 são ímpares, temos que $A^2 - DB^2$ tem de ser ímpar. Por hipótese, $xx_0 \equiv A^2 + B^2 \equiv 1 \pmod 4$. Como no item anterior, $x \equiv x_0 \pmod 4$.
- Módulo 8
  - Quando D é múltiplo de 8, os números ímpares n representados por F somente tomam uma das seguintes formas: $8k + 1$, $8k + 3$, $8k + 5$, $8k + 7$. O argumento é semelhante a trabalhar em módulo 4, pois $4 \mid 8$.
  - Quando $D \equiv 2 \pmod 8$, os restos dos números ímpares na divisão por 8 que se representam por F ou alternarão entre 1 e 7, ou alternarão entre 3 e 5. Tendo x, x_0 números ímpares, sabemos que $xx_0 = A^2 - DB^2 \equiv A^2 - 2B^2 \pmod 8$, o que força a que A seja ímpar (se A fosse par, teriamos xx_0 par e isso seria uma contradição). Assim $A^2 \equiv 1 \pmod 8$ e, por tentativas, concluímos que $DB^2 \equiv 0, 2 \pmod 8$, logo $xx_0 \equiv \pm 1 \pmod 8$. Para resolver esta congruência final, ou temos x, x_0 com a representação $8k \pm 1$ ou temos x, x_0 com a representação $8k \pm 3$.
  - Quando $D \equiv 6 \pmod 8$, os restos dos números ímpares na divisão por 8 representados por F ou alternarão entre 1 e 3, ou alternarão entre 5 e 7. O argumento é o mesmo que o anterior, considerando agora que $xx_0 = A^2 - DB^2 \equiv A^2 + 2B^2 \pmod 8$.

Exemplo 3.54
Vejamos os seguintes exemplos de formas quadráticas binárias módulo 8.

- *Seja* $F = (3, 1, 5)$ *de determinante* $-14 \equiv 2 \pmod 8$. *Pelo raciocínio anterior, todos os números ímpares representados por* F *deixarão o mesmo resto na divisão por* 8, *em particular os coeficientes extremos, pois* $F(1, 0) = a$ *e* $F(0, 1) = c$. *Logo, os números ímpares representados por* F *têm de deixar resto* ± 3 *na divisão por* 8.

- *Seja* $F = (5, 1, 7)$ *de determinante* $-34 \equiv 6 \pmod 8$. *Neste caso, também analisando os coeficientes extremos, vemos que os números ímpares representados por* F *têm de deixar resto* 5 *ou* 7 *na divisão por* 8.

A partir do artigo 230 de DA, Gauss começa a catalogar as formas quadráticas tendo por base estas relações encontradas como consequências do teorema no artigo 229. Vemos que os números ímpares representados por F estão intimamente relacionados com os divisores primos do determinante mas também com os números 4 e 8.

Definição 3.55 (Caráter)
Seja $F = (a, b, c)$ uma forma quadrática binária primitiva de determinante $D = b^2 - ac$ divisível por um primo p. O CARÁTER[1] (ou CARÁTER PARTICULAR) de F é um símbolo que ilustra as relações estudadas até agora e define-se do seguinte modo:

- Número primo p: Quando F só representa resíduos quadráticos módulo p, atribuimos o símbolo Rp. Caso F só represente não-resíduos quadráticos, atribuimos o símbolo Np.

- Potências de 2: 4 e 8. Este caráter representa-se com o símbolo χ_0.

    1. Quando F apenas representa números ímpares cujo resto na divisão por 4 seja 1, o símbolo atribuido será $[1, 4]$. De forma análoga, definimos os símbolos $[3, 4]$; $[1, 8]$; $[3, 8]$; $[5, 8]$; $[7, 8]$.
    2. Quando F somente representa números ímpares cujos restos na divisão por 8 alternam como vimos anteriormente, o símbolo a atribuir será [1 e $7, 8$] caso alternem entre 1 e 7 módulo 8. Analogamente, definimos os caracteres [3 e $5, 8$], [1 e $3, 8$], [5 e $7, 8$].

Observação 3.56 (Símbolo de Legendre e caracteres)
Gauss e Legendre definiram notações diferentes para indicar se um número x é resíduo quadrático módulo m. Legendre criou a notação que hoje conhecemos, mas Gauss usou esta notação que depois adaptou para a Teoria de Caracteres. Caso x fosse resíduo de m, denotaria xRm e caso fosse não-resíduo denotaria xNm. Do mesmo modo, podemos dizer que atribuimos a x os caracteres Rm ou Nm, respetivamente.

Proposição 3.57 (Caracteres e Coeficientes Extremos)
Seja $F = (a, b, c)$ uma forma quadrática binária de determinante D. Então, a e c terão os mesmos caracteres que F.

[1] A bem da uniformidade dentro da comunidade matemática, escolhemos grafar esta palavra deste modo, ainda que a crescente popularização de disciplinas como a Informática induzam a sua pronúncia a ser próxima de /carac'tére/, quando nos referimos a símbolos.

Demonstração. Suponhamos que D é divisível por p primo, ou $p = 4$, ou $p = 8$. Usando a observação 3.5, sabemos que $aF(x,y) = (ax+by)^2 - Dy^2$ e $cF(x,y) = (bx+cy)^2 - Dx^2$. Como p é divisor de D, vem que $aF(x,y) \equiv (ax^2+by)^2 \pmod{p}$ e $cF(x,y) \equiv (bx+cy)^2 \pmod{p}$. Deste modo, temos que $\left(\frac{aF(x,y)}{p}\right) = 1$. Logo, segue que $\left(\frac{a}{p}\right) = \left(\frac{F(x,y)}{p}\right)$. Analogamente para c.

Q.E.D.

Definição 3.58 (Caráter completo)
Seja F uma forma quadrática de determinante $D = \pm 2^{\alpha} p_0^{\alpha_0} p_1^{\alpha_1} \dots p_{m-1}^{\alpha_{m-1}}$, sendo p_m primos ímpares distintos, $\alpha \in \mathbb{N}$ e $m, \alpha_i \in \mathbb{N}_1$. O CARÁTER COMPLETO de F é o conjunto de todos os caracteres particulares de F associados aos primos divisores de D. Denotamo-lo por $\Gamma_F := \{\chi_0, \chi p_0, \chi p_1, \dots, \chi p_{m-1}\}$, sendo que χ pode ser R ou N, e χ_0 é o caráter que denota a relação de D com os módulos 4 ou 8.

Exemplo 3.59
Seja a forma $F = (10,3,17)$ *com determinante* $-161 = (-1)\cdot 7 \cdot 23$. *Sabemos que* 10 *se representa por* F, *o que nos permite calcular os caracteres com respeito a* 7 *e com respeito a* 23. *Como* 10 *é um não-resíduo quadrático módulo* 7, *todos os valores de* F *serão não-resíduos quadráticos módulo* 7, *pelo que lhe atribuimos o caráter* N7. *Do mesmo modo, atribuimos o caráter* N23. *Pelos módulos* 4 *e* 8, *sabemos que* $-161 \equiv 3 \pmod 4$, *logo todos os números ímpares* N *representados por* F *ou são todos* $N \equiv 1$ *módulo* 4 *ou são todos* $N \equiv 3$ *módulo* 4. *Como* $F(0,1) = 17 \equiv 1 \pmod 4$, *atribuimos-lhe o caráter* $[1,4]$. *Assim, a forma* F *tem o caráter completo* $\Gamma_F = \{[1,4], \text{N7}, \text{N23}\}$.

Após esta análise, Gauss considera todas as classes de equivalência de formas com determinante -161 e, após determinar a forma representante para cada classe, calcula o seu caráter completo exibindo assim a tabela, adaptada da tabela em ([Gau95], p.239):

Caráter completo	Formas representantes
$[1,4]$, R7, R23	$(1,0,161)$, $(2,1,81)$, $(9,1,18)$, $(9,-1,18)$
$[1,4]$, N7, N23	$(5,2,33)$, $(5,-2,33)$, $(10,3,17)$, $(10,-3,17)$
$[3,4]$, R7, N23	$(7,0,23)$, $(11,2,15)$, $(11,-2,15)$, $(14,7,15)$
$[3,4]$, N7, R23	$(3,1,54)$, $(3,-1,54)$, $(6,1,27)$, $(6,-1,27)$

Tabela 3.6: Caracteres completos para as formas quadráticas binárias com determinante -161

Podemos resumir a possível atribuição de um caráter χ_0 a uma forma, mediante uma tabela inspirada pela tabela em ([BK09], p.144). Sendo p_i primos ímpares, $\alpha, m \in \mathbb{N}$, temos:

Determinante	Possível χ_0
$D = \pm 2^{\alpha} \cdot 8 \cdot p_0 \dots p_{m-1}$	$[1,8]$,$[3,8]$,$[5,8]$,$[7,8]$
$D = \pm 4 \cdot p_0 \dots p_{m-1}$	$[1,4]$,$[3,4]$
$D = \pm 2 \cdot p_0 \dots p_{m-1}$	$[1$ e $7,8]$, $[3$ e $5,8]$ ou $[1$ e $3,8]$, $[5$ e $7,8]$
$D \equiv 3 \pmod 4$	$[1,4]$,$[3,4]$
$D \equiv 1 \pmod 4$	N/A

Tabela 3.7: Atribuição do caráter χ_0 em função da natureza do determinante

Definição 3.60 (Género)
Dizemos que duas formas F e G estão no mesmo género se têm o mesmo caráter completo.

Definição 3.61 (Forma Principal, Classe Principal, Género Principal)
Seja $D \in \mathbb{Z}$. A FORMA PRINCIPAL de determinante D define-se por $x^2 - Dy^2$, a classe da forma principal é chamada de CLASSE PRINCIPAL e o género da forma principal é chamado de GÉNERO PRINCIPAL.

Observação 3.62 (Caráter completo da Forma Principal)
Não será de mais ressalvar que o caráter completo da forma quadrática binária principal de determinante $D = \pm 2^{\alpha} p_0^{\alpha_0} p_1^{\alpha_1} \dots p_{m-1}^{\alpha_{m-1}}$ é $\Gamma_P = \{\chi_0, \mathrm{R}p_0, \mathrm{R}p_1, \dots, \mathrm{R}p_{m-1}\}$. Isto deve-se a que $x^2 - Dy^2 \equiv x^2 \pmod{p_i}$, para todo o primo divisor do determinante.

3.5 Artigo 233: Números característicos

No artigo 233 do DA, Gauss apresenta e desenvolve o conceito de *números característicos*. Este conceito será importantíssimo para o seu método de fatorização, pelo que, exporemos o artigo de Gauss na sua integra para as caracterizações que nos serão úteis.

Definição 3.63 (Números característicos)
Seja $F = (a, b, c) = ax^2 + 2bxy + cy^2$ uma forma quadrática primitiva. Sejam $m, W \in \mathbb{Z} \setminus \{0\}$ tal que $\mathrm{mdc}(m, W) = 1$. Se existem inteiros g, h tais que

$$g^2 \equiv aW \pmod{m}, \qquad gh \equiv bW \pmod{m}, \qquad h^2 \equiv cW \pmod{m},$$

então $(gx + hy)^2 \equiv g^2x^2 + 2ghxy + h^2y^2 \equiv W \cdot (ax^2 + 2bxy + cy^2) \equiv WF \pmod{m}$.
Neste caso, dizemos que WF é um resíduo quadrático[2] módulo m e $gx + hy$ é um valor da expressão $\sqrt{WF}$ módulo m. Assim, definimos que W é um NÚMERO CARACTERÍSTICO de F.

Exemplo 3.64
Sejam[3] $F = (3, 1, 54)$ *e* $m = 23$. *Como* $7^2 \equiv 3 \pmod{23}$, $7 \cdot 10 \equiv 1 \pmod{23}$ *e* $10^2 \equiv 54 \pmod{23}$, F *é um resíduo quadrático de* 23 *e* $7x + 10y$ *é um valor de* $\sqrt{3x^2 + 2xy + 54y^2}$ *módulo* 23.
Sejam $F = (10, 3, 17)$, $W = 5$ *e* $m = 23$. *Por contas semelhantes, chegamos à conclusão que* $5F$ *é um resíduo quadrático de* 23 *e* $2x - 4y$ *é um valor de* $\sqrt{5 \cdot (10x^2 + 6xy + 17y^2)}$ *módulo* 23.

Proposição 3.65 (Divisor do determinante)
Seja $F = (a, b, c)$ forma primitiva de determinante D. Caso WF seja um resíduo quadrático módulo m, m terá de ser um divisor de D.

Demonstração. Suponhamos que $gx + hy$ é um valor da expressão $\sqrt{WF}$ módulo m, ou seja,

$$g^2 \equiv aW \pmod{m}, \qquad gh \equiv bW \pmod{m}, \qquad h^2 \equiv cW \pmod{m}.$$

Como se tem $(bW)^2 \equiv (gh)^2 \equiv (aW) \cdot (cW) \equiv acW^2 \pmod{m}$ vem que $(b^2 - ac)W^2 \equiv 0 \pmod{m}$.
Como $\mathrm{mdc}(m, W) = 1$, temos que $(b^2 - ac) \equiv 0 \pmod{m}$ e assim $m \mid b^2 - ac$.

Q.E.D.

[2] Neste caso, estamos a confundir a forma quadrática com os valores que a mesma representa.
[3] Estamos a assumir que $W = 1$.

Proposição 3.66 (Caracteres)
Sejam $F = (a, b, c)$ forma primitiva de determinante D e $m = p^\alpha$, tal que $\alpha \in \mathbb{N}_1$ e p é primo. Caso WF seja um resíduo quadrático módulo m, o caráter particular de F com respeito a p será Rp se W é um resíduo quadrático módulo p e Np caso não o seja. Analogamente, caso $m = 4$, então o caráter particular de F com respeito a 4 será $[x, 4]$ caso $W \equiv x \pmod 4$, e caso $m = 8$, o caráter particular de F com respeito a 8 será $[x, 8]$ caso $W \equiv x \pmod 8$.

Demonstração. Suponhamos que $m = p^1$. Como F é primitiva, temos que p não divide a e c simultaneamente. Logo, como se tem $g^2 \equiv aW \pmod p$ e $h^2 \equiv cW \pmod p$, se W é resíduo quadrático, tanto a como c são resíduos quadráticos e se W é não-resíduo quadrático, a e c também serão não-resíduos quadráticos. Este argumento vale para quando m é uma potência de um primo p, com $\alpha \geqslant 2$, pois $p \mid m$.

Q.E.D.

O mais fascinante sobre esta proposição é que a afirmação recíproca também é verdadeira, e Gauss demonstra-o de seguida.

Proposição 3.67
Seja $D = b^2 - ac$ divisível por m, tal que $m = p^\alpha$ e $\alpha \in \mathbb{N}_1$ e p é um primo ímpar. Caso W seja um resíduo quadrático ou um não-resíduo quadrático de p, consoante o caráter de F com respeito a p seja Rp ou Np respetivamente, então WF será um resíduo quadrático de m.

Demonstração. Supondo que $p \nmid a$, aW será um resíduo de p e assim também de m. Tomemos g t.q. $g^2 \equiv aW \pmod m$ e $h \equiv \frac{bg}{a} \pmod m$. Então, $g^2 \equiv aW \pmod m$ e $ah \equiv bg \pmod m$.
Ou seja, $agh \equiv bg^2 \equiv abW \pmod m$ e $gh \equiv bW \pmod m$. Donde se conclui,

$$ah^2 \equiv bgh \equiv Wb^2 \equiv Wb^2 - W(b^2 - ac) \equiv acW \pmod m.$$

Ou seja $h^2 \equiv cW \pmod m$. Portanto, $gx + hy$ é um valor da expressão $\sqrt{WF} \pmod m$.
Caso $p \mid a$, então $p \nmid c$ e poderemos adaptar o argumento anterior.

Q.E.D.

Observação 3.68
Continuamos a considerar m um divisor do determinante D, prestando especial atenção aos casos $m = 4$ ou $m = 8$. Caso $m = 4$, se W se toma tal que $W \equiv x \pmod 4$, então WF será um resíduo quadrático de m caso $[x, 4]$ seja um caráter particular de F. Analogamente para $m = 8$.

Vimos que podiamos calcular os caracteres particulares de F ao analisar os seus coeficientes extremos. Podemos também fazer este cálculo usando W. Vejamos isto com um exemplo:

Exemplo 3.69
Sejam $F = (20, 10, 27)$ *e* $W = 3$. *Fazendo algumas contas, podemos ver que* $3(20, 10, 27)$ *é um resíduo quadrático de* 440. *Fatorizando, vem que* $440 = 5 \cdot 11 \cdot 8$. *Como* $\left(\frac{W}{5}\right) = -1$, *sabemos que o caráter com respeito a* 5 *será* N5. *Do mesmo modo, como* $\left(\frac{W}{11}\right) = 1$, *o caráter com respeito a* 11 *será* R11. *Finalmente, como* $W \equiv 3 \pmod 8$, *o caráter com respeito a* 8 *será* $[3, 8]$.

Proposição 3.70
Seja $F = (a, b, c)$ de determinante $D = b^2 - ac$. Suponhamos agora que mdc$(W, D) = 1$ e W tem os mesmos caracteres particulares atribuidos que F com respeito aos mesmos primos. Então, WF será um resíduo quadrático de D.

Demonstração. Podemos fatorizar $D = \pm p_0^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ em primos. Deste modo, usando a prop 3.67, WF será um resíduo quadrático de $p_i^{\alpha_i}$. Suponhamos que $u_i x + v_i y$ é um valor da expressão $\sqrt{WF} \pmod{p_i^{\alpha_i}}$. Para cada i, consideramos as congruências:

$$g^2 \equiv u_i^2 \equiv aW \pmod{p_i^{\alpha_i}}, \qquad gh \equiv u_i \cdot v_i \equiv bW \pmod{p_i^{\alpha_i}}, \qquad h^2 \equiv v_0^2 \equiv cW \pmod{p_i^{\alpha_i}}.$$

Deste modo, deduzimos que:

$$\begin{cases} g^2 \equiv aW \pmod{p_0^{\alpha_0} p_1^{\alpha_1} \dots p_n^{\alpha_n}} \\ gh \equiv bW \pmod{p_0^{\alpha_0} p_1^{\alpha_1} \dots p_n^{\alpha_n}} \\ h^2 \equiv cW \pmod{p_0^{\alpha_0} p_1^{\alpha_1} \dots p_n^{\alpha_n}} \end{cases} \iff \begin{cases} g^2 \equiv aW \pmod{D} \\ gh \equiv bW \pmod{D} \\ h^2 \equiv cW \pmod{D}. \end{cases}$$

Ou seja, WF é resíduo quadrático de D.

Q.E.D.

Lema 3.71
Se W é um número característico de uma forma primitiva F com determinante D, todos os números congruentes a W módulo D também serão números característicos de F.

Observação 3.72 (Números característicos triviais)
Sabemos que 1 é sempre um resíduo quadrático de qualquer forma, classe ou género, pelo que uma forma é sempre um resíduo do seu determinante.

Observação 3.73 (Mesmo género, mesmos números característicos)
Todas as formas numa mesma classe ou de classes diferentes no mesmo género têm os mesmos números característicos. De tal modo, encontrando um número característico para uma forma F, poderemos atribui-lo a toda a classe e género aos quais pertença F.

Esta última observação consegue deduzir-se a partir das proposições 3.66 e 3.70. Esta observação será de suma importância na geração de resíduos quadráticos.

Com os resultados teóricos desenvolvidos até agora, já temos os meios necessários para entender a segunda técnica de Gauss para gerar resíduos quadráticos. Antes de avançar para o último conceito, se quiser, o leitor já pode ver a aplicação desta teoria no início do capítulo 4. O próximo conceito será necessário para se entender a terceira e última técnica que Gauss desenvolve para gerar resíduos quadráticos.

3.6 Composição de Formas Quadráticas

A partir do artigo 234 de DA, Gauss começa a desenvolver a Composição de Formas. O seu objetivo central é criar uma operação que se comporte como a multiplicação de polinómios, mas

de forma a que este produto de formas quadráticas seja também uma forma quadrática. Talvez tenha sido inspirado pelas identidades de Brahmagupta (lema 1.46) e pelo facto de como cada forma quadrática se pode transformar numa expressão com o formato de cada uma das parcelas do lado esquerdo destas identidades (observação 3.5). Esta teoria é extensa com uma exposição bastante técnica e é um dos conceitos mais complicados de todos os abarcados pelo *Disquisitiones Arithmeticae*. No artigo 235, Gauss começa a sua exposição com a seguinte definição.

Definição 3.74 (Forma composta)
Seja $F(X,Y) = AX^2 + 2BXY + CY^2$ uma forma quadrática binária, e suponhamos que $F(X,Y)$ se pode escrever como o produto de outras duas formas $f_0(x_0,y_0) = a_0x_0^2 + 2b_0x_0y_0 + c_0y_0^2$ e $f_1(x_1,y_1) = a_1x_1^2 + 2b_1x_1y_1 + c_1y_1^2$ após aplicarmos a seguinte mudança de coordenadas:

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix} \begin{pmatrix} x_0x_1 \\ x_0y_1 \\ y_0x_1 \\ y_0y_1 \end{pmatrix}.$$

Denotando

$$A_1 = a_{11}a_{22} - a_{12}a_{21}, \qquad A_2 = a_{11}a_{23} - a_{13}a_{21}, \qquad A_3 = a_{11}a_{24} - a_{14}a_{21},$$

$$A_4 = a_{12}a_{23} - a_{13}a_{22}, \qquad A_5 = a_{12}a_{24} - a_{14}a_{22}, \qquad A_6 = a_{13}a_{24} - a_{14}a_{23}.$$

Se $\text{mdc}(A_1,A_2,A_3,A_4,A_5,A_6) = 1$, F é a forma composta por f_0 e f_1.

Observação 3.75
Se considerarmos a forma $F(X,Y) = X^2 - DY^2$ e a substituição

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & D \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_0x_1 \\ x_0y_1 \\ y_0x_1 \\ y_0y_1 \end{pmatrix},$$

recuperamos a identidade de Brahmagupta demonstrada no lema 1.46.

Observação 3.76 (Nota histórica)
Ninguém anterior a Gauss tratara este tema, tal como o próprio afirmou no artigo 234. Deste modo, o seu raciocínio original, constando dos artigos numerados entre 234 e 251 de [Gau95], é demasiado longo e técnico para ser exposto nesta dissertação. Contudo, Gustav Dirichlet conseguiu simplificar os trabalhos de Gauss grandemente e criou uma maneira mais clara para determinar a composição de 2 formas quadráticas arbitrárias com o mesmo determinante, baseando-se num caso particular contemplado no DA, no artigo 243.

Na subsecção seguinte, expomos uma versão atualizada da composição de formas quadráticas usando o conceito de FORMAS UNIDAS de Dirichlet adaptado à definição original de Gauss. Para este efeito, baseámo-nos nos trabalhos [Bue89], [BK09] e [Fel18], dando-lhes um toque pessoal para recontextualizar algumas deduções.

3.6.1 Operação de Composição

Definição 3.77 (Formas Unidas)
Sejam $F_0 = (a_0, b_0, c_0)$ e $F_1 = (a_1, b_1, c_1)$ formas quadráticas tais que $\det(F_0) = \det(F_1) = D$. Dizemos que F_0 e F_1 são FORMAS UNIDAS caso $\text{mdc}(a_0, a_1, b_0 + b_1) = 1$.

Definição 3.78 (Formas Concordantes)
Sejam $F_0 = (a_0, b_0, c_0)$ e $F_1 = (a_1, b_1, c_1)$ formas quadráticas tais que $\det(F_0) = \det(F_1) = D$. Dizemos que F_0 e F_1 são FORMAS CONCORDANTES caso se verifique

$$a_0 a_1 \neq 0, \qquad b_0 = b_1, \qquad a_0 \mid c_1, \qquad a_1 \mid c_0.$$

O nosso objetivo ao longo desta subsecção será reduzir o problema de composição de duas formas quadráticas binárias arbitrárias com o mesmo determinante D ao problema de composição de duas formas quadráticas binárias unidas e concordantes, uma vez que este caso é mais simples de se tratar. Para tal efeito, começamos por estabelecer uns resultados intermédios.

Lema 3.79 (Coprimalidade)
Seja $F(x, y) = ax^2 + 2bxy + cy^2$ uma forma quadrática binária primitiva e seja $A \in \mathbb{Z} \setminus \{0, \pm 1\}$. Então, existe um inteiro N representado por F t.q. $\text{mdc}(N, A) = 1$

Demonstração. Seja p divisor de A. Consideremos $S = \{(1,0), (1,1), (0,1)\}$ e seja $(\alpha_p, \gamma_p) \in S$ tal que $F(\alpha_p, \gamma_p)$ e p são coprimos. Este par existe pois F é primitiva e p não pode dividir simultaneamente $f(1,0) = a,\ f(0,1) = c,\ f(1,1) = a + 2b + c$.

Consideremos a fatorização em primos de $A = \pm p_0^{\beta_0} p_1^{\beta_1} p_2^{\beta_2} \ldots$ e para cada primo p_i criamos o par (α_i, γ_i) nas condições acima expostas. De seguida, resolvemos os sistemas de congruências,

$$\begin{cases} \alpha \equiv \alpha_0 \pmod{p_0} \\ \alpha \equiv \alpha_1 \pmod{p_1} \\ \alpha \equiv \alpha_2 \pmod{p_2} \\ \ldots \end{cases} \quad \text{e} \quad \begin{cases} \gamma \equiv \gamma_0 \pmod{p_0} \\ \gamma \equiv \gamma_1 \pmod{p_1} \\ \gamma \equiv \gamma_2 \pmod{p_2} \\ \ldots \end{cases}.$$

Por construção, $N := F(\alpha, \gamma)$ e A são coprimos. Caso α e γ não sejam coprimos, consideramos $\alpha^- = \frac{\alpha}{\text{mdc}(\alpha,\gamma)}$ e $\gamma^- = \frac{\gamma}{\text{mdc}(\alpha,\gamma)}$. Como $f(\alpha^-, \gamma^-)$ divide $f(\alpha, \gamma)$, então $f(\alpha^-, \gamma^-)$ e A são coprimos. Q.E.D.

Lema 3.80 (Lema do Coeficiente Médio)
Sejam $F_0^* = (a_0^*, b_0^*, c_0^*)$ e $F_1^* = (a_1^*, b_1^*, c_1^*)$ duas formas quadráticas unidas de determinante D. Seja S o sistema de congruências seguinte:

$$\begin{cases} B \equiv b_0^* \pmod{a_0^*} \\ B \equiv b_1^* \pmod{a_1^*}. \end{cases}$$

Então, o sistema de congruências S tem uma solução única módulo $\text{mmc}(a_0^*, a_1^*)$.

Demonstração. Consideremos o sistema de congruências anterior. Como as formas F_0^* e F_1^* têm o mesmo determinante, $D = {b_0^*}^2 - a_0^* c_0^* = {b_1^*}^2 - a_1^* c_1^*$, sabemos que

$$(b_0^* + b_1^*)(b_0^* - b_1^*) = a_0^* c_0^* - a_1^* c_1^*.$$

Deste modo, $d = \text{mdc}(a_0^*, a_1^*)$ divide o lado direito da última equação, pelo que também deve dividir o lado esquerdo. Agora como as formas são unidas, $\text{mdc}(a_0^*, a_1^*, b_0^* + b_1^*) = 1$, logo $d \nmid (b_0^* + b_1^*)$. Assim, $d \mid b_0^* - b_1^*$.

Pela identidade de Bézout, é possível escrever $b_0^* - b_1^* = -a_0^* k + a_1^* t$ para certos $k, t \in \mathbb{Z}$. Podemos usar esta igualdade para construir uma solução para o sistema,

$$B = b_0^* + a_0^* k = b_1^* + a_1^* t.$$

Tomando outra solução $B' = b_0^* + a_0^* k' = b_1^* + a_1^* t'$, vem que

$$B' - B = a_0^*(k' - k) = a_1^*(t' - t).$$

Vem que $B' - B$ é múltiplo de a_0^* e de a_1^*, logo terá de o ser de $\text{mmc}(a_0^*, a_1^*)$. Logo, a solução é única módulo $\text{mmc}(a_0^*, a_1^*)$.

Q.E.D.

Proposição 3.81 (Conversão de formas unidas para formas concordantes)
Sejam $F_0^* = (a_0^*, b_0^*, c_0^*)$ e $F_1^* = (a_1^*, b_1^*, c_1^*)$ formas quadráticas unidas de determinante D, tais que $\text{mdc}(a_0^*, a_1^*) = 1$. Então, existem formas concordantes $F_0' = (a_0', b_0', c_0')$ e $F_1' = (a_1', b_1', c_1')$ tais que

$$(a_0^*, b_0^*, c_0^*) \leftrightarrow_P (a_0', b_0', c_0') \qquad \text{e} \qquad (a_1^*, b_1^*, c_1^*) \leftrightarrow_P (a_1', b_1', c_1'),$$

sendo $a_0^* = a_0'$, $a_1^* = a_1'$.

Demonstração. Sejam $F_0^* = (a_0^*, b_0^*, c_0^*)$ e $F_1^* = (a_1^*, b_1^*, c_1^*)$ formas quadráticas unidas de determinante D. Tomemos os inteiros k, l vistos na demonstração do lema anterior para criar as seguintes matrizes

$$M_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \qquad \text{e} \qquad M_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

Pelo lema anterior, fazendo mudanças de coordenadas com estas matrizes, vemos que F_0 implica a forma quadrática $F_0^*(x, y) = a_0^* x^2 + 2Bxy + \mu_k y^2$ usando a matriz M_k, e F_1 implica a forma quadrática $F_1^*(x, y) = a_1^* x^2 + 2Bxy + \mu_t y^2$ usando a matriz M_t, para certos $\mu_k, \mu_t \in \mathbb{Z}$.

Como $\det(M_k) = \det(M_t) = 1$, sabemos que esta implicação é uma equivalência própria. Logo, como F_0^* e F_1^* têm o mesmo determinante, sabemos que F_0' e F_1' terão o mesmo determinante. Assim, sabemos que $a_0^* \mu_k = a_1^* \mu_t$. Como $\text{mdc}(a_0^*, a_1^*) = 1$, existe C tal que $\mu_k = a_1^* C$ e $\mu_t = a_0^* C$. Portanto, as formas $F_0' = (a_0^*, B, a_1^* C)$ e $F_1' = (a_1^*, B, a_0^* C)$ são concordantes.

Q.E.D.

Observação 3.82
Notemos que ter $\mathrm{mdc}(a_0^*, a_1^*) = 1$ é suficiente para que F_0^* e F_1^* sejam formas quadráticas unidas, pois $\mathrm{mdc}(a_0^*, a_1^*, b_0^* + b_1^*) = \mathrm{mdc}(\mathrm{mdc}(a_0^*, a_1^*), b_0^* + b_1^*)$. Caso tenhamos que $\mathrm{mdc}(a_0^*, a_1^*) = 1$, é útil observar que $C = C \cdot \mathrm{mdc}(a_0^*, a_1^*) = \mathrm{mdc}(a_0^* C, a_1^* C)$, para certo $C \in \mathbb{Z}$.

A última proposição permite-nos equivaler um par de formas quadráticas unidas a um par de formas quadráticas unidas e concordantes. Após os últimos resultados, estamos finalmente prontos para descrever então o processo de composição de Dirichlet.

Composição de Dirichlet
Sejam $F_0 = (a_0, b_0, c_0)$ e $F_1 = (a_1, b_1, c_1)$ duas formas quadráticas binárias com o mesmo determinante que queremos compor. A ideia geral deste processo é fazer transformações de equivalência para obter, numa primeira fase, um par de formas quadráticas unidas e, numa segunda fase, um par de formas quadráticas concordantes e unidas.

1. Se a_0 e a_1 forem t.q. $\mathrm{mdc}(a_0, a_1) = 1$, pela observação anterior, sabemos que F_0 e F_1 são formas quadráticas unidas e passamos ao próximo item. Caso contrário, encontramos um par de formas quadráticas binárias equivalentes F_0^* e F_1^* com coeficientes iniciais coprimos. Baseando-nos no lema 3.79, tomemos $\alpha, \gamma \in \mathbb{Z}$ coprimos de forma a que $F_0(\alpha, \gamma)$ e a_1 sejam relativamente primos. Para se ter uma equivalência, consideramos $\beta, \delta \in \mathbb{Z}$ tal que $\alpha\delta - \beta\gamma = 1$. Então $F_0^* = F_0(\alpha x + \beta y, \gamma x + \delta y) = (a_0^*, b_0^*, c_0^*)$. Com esta mudança de coordenadas, F_0 e F_0^* são propriamente equivalentes. Sabemos que $a_0^* = F_0^*(1, 0) = F_0(\alpha, \gamma)$ é coprimo com $a_1 = F_1(1, 0)$ e assim temos um par de formas quadráticas com coeficientes iniciais coprimos. Naturalmente, definimos $F_1^* := F_1$.

2. Pela observação 3.82, como as formas F_0^* e F_1^* são unidas, usamos a proposição 3.81 para as equivaler às formas quadráticas concordantes $F_0' = (a_0^*, B, a_1^* C),\ F_1' = (a_1^*, B, a_0^* C)$.

Tendo as formas $(a_0^*, B, a_1^* C), (a_1^*, B, a_0^* C)$ tais que $\mathrm{mdc}(a_0^*, a_1^*) = 1$, usamos a seguinte identidade:

$$(a_0^* x_0^2 + 2Bx_0y_0 + a_1^* C y_0^2)(a_1^* x_1^2 + 2Bx_1y_1 + a_0^* C y_1^2) = a_0^* a_1^* X^2 + 2BXY + CY^2 \tag{3.9}$$

Este produto é justificado pela mudança de coordenadas,

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_0^* & a_1^* & 2B \end{pmatrix} \begin{pmatrix} x_0x_1 \\ x_0y_1 \\ y_0x_1 \\ y_0y_1 \end{pmatrix}.$$

Esta última forma é a Forma composta por F_0 e F_1 e denotamo-la por $F_0 \odot F_1$. Caso $F_0 \odot F_1$ não seja reduzida, basta aplicar um dos algoritmos de redução já vistos.

Observação 3.83
A composição de Dirichlet é uma simplificação dos estudos de Gauss. Poderíamos fazer a composição de duas formas usando o processo original, mas seria mais extenso. Este processo transforma o problema de composição de formas num problema de composição ao nível das

classes de equivalência das mesmas formas, pois procuramos outros representantes nas classes das formas a compôr que satisfaçam a identidade (3.9) ao executarmos os dois passos anteriores.

Exemplo 3.84
Suponhamos que queremos compôr as formas quadráticas[4] $F_0 = (2, 5, 9)$ *e* $F_1 = (2, 5, 9)$. *Consideremos* a_0, b_0, c_0 *os coeficientes de* F_0 *e* a_1, b_1, c_1 *os coeficientes de* F_1.

1. *Como estas formas não são unidas, usamos o lema* 3.79 *para as equivaler a formas quadráticas unidas. Pelo lema, de entre os pares* $(0,1),(1,1),(1,0)$, *temos que* $\mathrm{mdc}(F_0(0,1), a_1) = 1$. *Como* a_1 *é primo, pelo lema 3.79, só temos de considerar um par de congruências. Isto significa que podemos tomar* $\alpha = 0,\ \gamma = 1$. *Como queremos que* $\alpha\delta - \beta\gamma = 1$, *podemos ter* $\beta = -1, \delta = 0$. *Fazendo assim a mudança de coordenadas de* F_0*:*

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 5 \\ 5 & 9 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 9 & -5 \\ -5 & 2 \end{pmatrix}.$$

   As formas $F_0^* = (9, -5, 2)$ *e* $F_1^* = (2, 5, 9)$ *já são unidas, logo passamos ao passo seguinte.*

2. *Queremos encontrar formas concordantes* F_0' *e* F_1' *propriamente equivalentes a* F_0^* *e* F_1^*, *respetivamente. Para o coeficiente médio, pelo lema* 3.80, *resolvemos o sistema de congruências*

$$\begin{cases} B \equiv -5 \pmod 9 \\ B \equiv 5 \pmod 2 \end{cases}$$

   Vem que $B \equiv 13 \pmod{18}$ *e assim* $13 = -5 + 9 \cdot 2 = 5 + 2 \cdot 4$. *Fazendo uma mudança de coordenadas a* F_0^* *e a* F_1^* *respetivamente:*

$$F_0 : \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 9 & -5 \\ -5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 13 \\ 13 & 18 \end{pmatrix} \qquad e \qquad F_1 : \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}\begin{pmatrix} 2 & 5 \\ 5 & 9 \end{pmatrix}\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 13 \\ 13 & 81 \end{pmatrix}.$$

   Já temos assim as formas quadráticas concordantes $F_0' = (9, 13, 18)$ *e* $F_1' = (2, 13, 81)$.

Agora, basta aplicar a identidade 3.9 *para obtermos a forma composta*

$$F_0 \odot F_1 = 18X^2 + 26XY + 9Y^2.$$

Esta forma não é reduzida, por isso, podemos reduzi-la à forma

$$F_r = X^2 + 4XY - 3Y^2 = (1, 2, -3).$$

Só nos falta verificar um detalhe importante. Até agora, definimos a operação de composição de formas quadráticas baseando-nos nas classes de equivalência a que pertenciam cada uma das formas. No entanto, é preciso entender se obteriamos o mesmo resultado se escolhêssemos outros representantes da mesma classe. Faremos isso de seguida.

[4] Não é necessário que as formas quadráticas sejam iguais, só precisam de ter o mesmo determinante. Escolhemos tomá-las iguais, para nos obrigar a ter de executar o primeiro passo na composição de Dirichlet.

Lema 3.85 (Gauss)
Sejam $F = (a, b, c)$ e $G = (d, e, f)$ formas quadráticas com o mesmo determinante. Deste modo, as formas F e G são equivalentes se e só se existirem inteiros α e γ tais que:

1. $a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = d$.
2. $a\alpha + (b + e)\gamma \equiv 0 \pmod{d}$.
3. $(b - e)\alpha + c\gamma \equiv 0 \pmod{d}$.

Demonstração. Este resultado segue naturalmente da observação 3.18.

Q.E.D.

Teorema 3.86 (Composição de classes)
Se F_0^* e F_1^* são formas quadráticas unidas e existem formas quadráticas unidas F_2^* e F_3^* tais que $F_0^* \leftrightarrow_P F_2^*$ e $F_1^* \leftrightarrow_P F_3^*$, então,

$$F_0^* \odot F_1^* \leftrightarrow_P F_2^* \odot F_3^*.$$

Demonstração. Esta demonstração foi adaptada de [Bue89]. Pela proposição 3.81, devido a serem equivalentes, podemos tomar as formas unidas a serem também concordantes:

$$F_0^* = (a_0^*, B, a_1^* C), \qquad F_1^* = (a_1^*, B, a_0^* C), \qquad F_2^* = (m_0^*, N, m_1^* L), \qquad F_3^* = (m_1^*, N, m_0^* L).$$

Pelo lema anterior, como $F_0^* \leftrightarrow_P F_2^*$ e $F_1^* \leftrightarrow_P F_3^*$, respetivamente, sabemos que têm de existir inteiros x_0, y_0, x_1, y_1 tais que:

$$\begin{cases} a_0^* x_0^2 + 2Bx_0y_0 + a_1^* C y_0^2 = m_0^* \\ a_0^* x_0 + (B + N)y_0 \equiv 0 \pmod{m_0^*} \\ (B - N)x_0 + a_1^* C y_0 \equiv 0 \pmod{m_0^*} \end{cases} \qquad \begin{cases} a_1^* x_1^2 + 2Bx_1y_1 + a_0^* C y_1^2 = m_1^* \\ a_1^* x_1 + (B + N)y_1 \equiv 0 \pmod{m_1^*} \\ (B - N)x_1 + a_0^* C y_1 \equiv 0 \pmod{m_1^*} \end{cases}$$

Queremos encontrar inteiros X e Y tal que:

$$\begin{cases} a_0^* a_1^* X^2 + BXY + CY^2 = m_0^* m_1^* \\ a_0^* a_1^* X + (B + N)Y \equiv 0 \pmod{m_0^* m_1^*} \\ (B - N)X + CY \equiv 0 \pmod{m_0^* m_1^*} \end{cases}$$

Fazendo o produto das duas igualdades nos sistemas anteriores como na equação (3.9), reparamos que temos a equação desejada se $X = x_0x_1$ e $Y = a_0^* x_0y_1 + a_1^* x_1y_0 + (B + N)y_0y_1$. Vamos assumir estas representações para X e Y. Agora, sabemos que as formas são equivalentes, por isso, os determinantes são iguais e assim

$$B^2 - a_0^* a_1^* C = N^2 - m_0^* m_1^* L \implies B^2 - N^2 \equiv a_0^* a_1^* C \pmod{m_0^* m_1^*}.$$

Portanto, podemos fazer o cálculo direto seguinte, provamos a primeira congruência.

$$0 \equiv \left(a_0^* x_0 + y_0(B + N)\right)\left(a_1^* x_1 + y_1(B + N)\right) \equiv a_0^* a_1^* X + Y(B + N) \pmod{m_0^* m_1^*}.$$

Para provar a segunda congruência, podemos escrever $(B-N)X+CY \equiv U \pmod{m_0^* m_1^*}$, de forma a concluir que $U \equiv 0 \pmod{m_0^* m_1^*}$.
A ideia é usar as congruências presentes nas condições de equivalência dos sistemas anteriores. Fazendo algumas das combinações possíveis, obtemos as quatro congruências seguintes:

$$\begin{cases} \left((B-N)x_0 + a_1^* C y_0\right)\left(a_1^* x_1 + (B+N)y_1\right) \equiv a_1^* U \pmod{m_0^* m_1^*} \\ \left(a_0^* x_0 + (B+N)y_0\right)\left((B-N)x_1 + a_0^* C y_1\right) \equiv a_0^* U \pmod{m_0^* m_1^*} \\ \left((B-N)x_0 + a_1^* C y_0\right)\left((B-N)x_1 + a_0^* C y_1\right) \equiv (B-N)U \pmod{m_0^* m_1^*} \\ C\left(a_1^* x_1 + (B+N)y_1\right)\left(a_0^* x_0 + (B+N)y_0\right) \equiv (B+N)U \pmod{m_0^* m_1^*} \end{cases}$$

Em todos estes produtos, ambas as expressões a multiplicar são congruentes com 0. Como tomámos formas quadráticas unidas, segue-se que $U \equiv 0 \pmod{m_0^* m_1^*}$. Logo, provámos a segunda congruência,

$$U \equiv (B-N)X + CY \equiv 0 \pmod{m_0^* m_1^*}.$$

Q.E.D.

Deste modo, provamos que a composição de 2 formas não depende das formas, mas sim das classes em que se inserem.

Teorema 3.87 (Gauss)
O conjunto das classes de formas quadráticas de determinante D forma um grupo abeliano finito, com a operação de composição definida acima. A identidade do grupo é a classe principal, o inverso de uma classe é a classe da forma oposta.

Para a presente dissertação, apenas nos será relevante compreender como calcular a composição de formas e as implicações que esta operação acarreta para a forma quadrática resultante. Uma vez que a demonstração deste teorema impressionante não é totalmente necessária para entender o trabalho de Gauss, escolhemos deixá-la omissa.

Observação 3.88 (Artigos 154 e 229, DA)
Ainda que deixemos omissa a demonstração, é importante entender que os cálculos efetuados nos teoremas 3.6 e 3.53 podem ser explicados à luz da composição de formas. Por exemplo, no teorema 3.6 fazemos a multiplicação das formas $f(m,n) = am^2 + 2bmn + cn^2$ e $f^*(\nu,\mu) = a\nu^2 - 2b\mu\nu + c\mu^2$. Sabemos que estas formas terão o mesmo determinante e, como são mutuamente opostas, não são propriamente equivalentes e assim estarão em classes distintas. O anterior teorema prevê que $f \odot f^*$, a forma composta por f e f^*, seja a forma principal $X^2 - DY^2$. Ora, ao observarmos a forma resultante na equação (3.2), temos exatamente a forma pretendida pondo $X = \mu(mb+nc) - \nu(ma+nb)$ e $Y = m\mu + n\nu$. Do mesmo modo, o cálculo feito no artigo 229 pode reinterpretar-se como a composição de uma forma com ela mesma.

3.6.2 Género e Potências de Classes

A última subsecção extensivamente trabalhada serviu o único propósito de mostrar que existe uma operação entre formas quadráticas binárias e que o conjunto das formas quadráticas com um mesmo determinante é fechado para esta operação, generalizando assim identidades como as identidades de Brahmagupta. Nesta subsecção recorremos a [BK09] e voltamos a basear-nos nos trabalhos de Gauss.

A partir da identidade (3.9) conseguimos perceber que a composição de formas quadráticas binárias comporta-se como um produto de formas quadráticas, ao qual equivale a outra forma quadrática. Sejam F e G um par de formas quadráticas binárias.

1. Seja $F^* = (a_0^*, B, a_1^* C)$ e $G^* = (a_1^*, B, a_0^* C)$ um par de formas quadráticas tais que $F \leftrightarrow_P F^*$, $G \leftrightarrow_P G^*$, e $\mathrm{mdc}(a_0^*, a_1^*) = 1$. Tomemos os inteiros N, P tais que $N = F(t,u)$ e $P = G(v,w)$. Como temos a equivalência entre formas, sabemos também que têm de existir $t^*, u^*, v^*, w^* \in \mathbb{Z}$ tais que $F^*(t^*, u^*) = N$ e $G^*(v^*, w^*) = P$.

2. Sendo assim, temos que $F(t,u) \odot G(v,w) = F^*(t^*, u^*) G^*(v^*, w^*) = NP$. Pela identidade (3.9), sabemos que têm de existir $x, y \in \mathbb{Z}$ tal que $H(x,y) = (F \odot G)(x,y) = NP$.

Em suma, podemos dizer que se F representa um inteiro N e G representa um inteiro P, então a forma composta $F \odot G$ tem de representar NP.

Definição 3.89 (Potência de uma forma)
Devido às semelhanças da composição de formas com a multiplicação, definimos POTÊNCIA DE UMA FORMA como a composição de uma forma com ela mesma. Isto quererá dizer que $F \odot F := F^2$, $F \odot F^2 := F^3$, e assim por diante

A ideia central do próximo resultado é estabelecer que as potências de uma forma quadrática binária podem pertencer apenas a um de dois géneros: o género a que F pertence e o género principal. Recebe algumas vezes o nome de "Teorema do Género Principal", como em ([BK09]).

Teorema do Género Principal

Seja F uma forma quadrática binária de determinante D cuja fatorização em primos é $D = \pm 2^{\alpha} p_0^{\alpha_0} p_1^{\alpha_1} \dots p_n^{\alpha_n}$, tal que $n, \alpha \in \mathbb{N}$ e $\alpha_i \in \mathbb{N}_1$ e p_i são números primos ímpares distintos. Suponhamos que o caráter completo de F é $\Gamma_F = \{\chi_0, \chi p_0, \chi p_1, \dots, \chi p_n\}$ em que χ pode ser R ou N e χ_0 é o caráter que diz respeito à maior potência de 2 que divide o determinante. Consideremos L, M, N representados por F, coprimos com o determinante D. O seguinte raciocínio foi adaptado de [BK09] e do artigo 246 do DA.

Divisores primos ímpares

Seja p_i um divisor primo ímpar do determinante. Como são representados por F, M e N têm o mesmo caráter χp_i. Usando o símbolo de Legendre, isto significa que

$$\left(\frac{M}{p_i}\right) = \left(\frac{N}{p_i}\right).$$

Donde concluímos que

$$\left(\frac{M}{p_i}\right)\left(\frac{N}{p_i}\right) = \left(\frac{MN}{p_i}\right) = 1.$$

Portanto, a MN atribuímos o caráter $\mathrm{R}p_i$. A partir do que estudámos anteriormente, sabemos que MN é representado por F^2. Isto significa que o caráter que atribuimos a F^2 também será $\mathrm{R}p$. Como tanto M, N e p_i foram tomados arbitrários, podemos repetir o argumento para todos os divisores primos do determinante e chegamos à conclusão que $A = \{\mathrm{R}p_0, \mathrm{R}p_1, \ldots, \mathrm{R}p_n\}$ é um subconjunto do caráter completo de F^2. Considerando L também representado por F, temos que $L\chi p_i$. Deste modo,

$$\left(\frac{M}{p_i}\right) = \left(\frac{N}{p_i}\right) = \left(\frac{L}{p_i}\right).$$

O que significa,

$$\left(\frac{MN}{p_i}\right) = \left(\frac{LN}{p_i}\right) = \left(\frac{LM}{p_i}\right) = 1.$$

Portanto,

$$\left(\frac{LMN}{p_i}\right) = \left(\frac{L}{p_i}\right)\left(\frac{MN}{p_i}\right) = \left(\frac{L}{p_i}\right) \cdot 1 = \left(\frac{L}{p_i}\right).$$

Deste cálculo, atribuimos a LMN e a L o caráter χp_i. Por conseguinte, como LMN é representado por F^3, de forma análoga atribuímos o caráter χp_i à forma F^3, como se fez para a forma F. A partir deste argumento, podemos afirmar que coincidirão todos os caracteres particulares de F^3 e F com respeito a divisores primos ímpares do determinante. Ou seja, $B = \{\chi p_0, \chi p_1, \ldots, \chi p_n\}$ será um subconjunto do caráter completo de F^3.

Finalizando, quanto aos divisores primos ímpares do determinante, podemos generalizar os cálculos anteriores, de modo a chegar a uma conclusão importante.

Proposição 3.90 (Caráter Completo Ímpar das Potências)
Seja F uma forma quadrática binária de determinante D com fatores primos ímpares distintos $p_0, p_1, p_2, \ldots, p_n$.

- As potências pares de F terão todas o mesmo subconjunto $A = \{\mathrm{R}p_0, \mathrm{R}p_1, \ldots, \mathrm{R}p_n\}$ de Γ_P, o caráter completo principal.
- As potências ímpares de F também partilharão o subconjunto $B = \{\chi p_0, \chi p_1, \ldots, \chi p_n\}$ de Γ_F, o caráter completo de F.

Com esta proposição estabelecida, só nos falta demonstrar como se comportam os caracteres χ_0 para concluir o resultado pretendido.

Potências de 2: Caráter χ_0
Estabelecemos antes que o género de uma forma quadrática apenas terá um caráter relacionado com uma potência de 2, caso $D \not\equiv 1 \pmod 4$. Para esta análise, o objetivo continua a ser mostrar que apenas atribuímos dois caracteres, não necessariamente distintos, às potências de F, um às potências ímpares e outro às potências pares. Repetiremos o argumento anterior, pelo que será

mais simples dividir o raciocinio por duas fases

$$D \equiv 0, 3 \pmod 4 \qquad \text{e} \qquad D \equiv \pm 2 \pmod 8.$$

Numa primeira fase, suponhamos que $D \equiv 0, 3 \pmod 4$. Logo, F terá um de dois caracteres $[1, 4]$, $[3, 4]$, como vimos na secção 3.4. Sendo M, N representados por F, concluímos que MN se representa por F^2 e, analisando o caráter atribuido a F, vemos que $MN \equiv 1 \pmod 4$. Isto significa que a F^2 atribuimos o caráter $[1, 4]$. Sendo L representado por F, vemos que $LMN \equiv L \pmod 4$. Donde concluimos que a F^3 atribuimos o mesmo caráter que a F.

Numa segunda fase, temos somente o caso em que $D \equiv \pm 2 \pmod 8$. Neste caso, sabemos que os valores de F módulo 8 alternarão entre dois valores mediante o caráter atribuído. Uma vez que o argumento usado continua a ser o mesmo, como há somente uma subtileza menor neste caso, apenas exporemos o caso em que $D \equiv 2 \pmod 8$.

Neste caso, sabemos que o caráter atribuído, ou é [1 e 7, 8], ou é [3 e 5, 8]. Portanto, os valores de F alternarão entre, ou 1 e 7 módulo 8, ou 3 e 5 módulo 8. Suponhamos que os valores de F alternam entre 3 e 5 módulo 8.
Caso M, N tenham o mesmo resto na divisão por 8, então vem que $MN \equiv 1 \pmod 8$. Caso tenham restos diferentes, então $MN \equiv 7 \pmod 8$. Do mesmo modo, devido a que MN se representa por F^2, o caráter atribuido a F^2 é [1 e 7, 8].
Consideremos agora L representado por F. Se $L \equiv 3 \pmod 8$, vem que $LMN \equiv 3 \pmod 8$ ou $LMN \equiv 5 \pmod 8$. Analogamente para $L \equiv 5 \pmod 8$. Ou seja, o caráter atribuido a F^3 é [3 e 5, 8] e assim é o mesmo caráter que o atribuido a F. Fazendo as contas para o caso em que os valores de F alternam entre 1 e 7 módulo 8, os resultados seriam que o caráter atribuido a F^2 é [1 e 7, 8] e o caráter atribuido a F^3 seria [1 e 7, 8].

Após os últimos parágrafos, provámos a seguinte proposição.

Proposição 3.91 (Caráter particular χ_0)
Seja F uma forma quadrática binária de determinante D. Quando $D \not\equiv 1 \pmod 4$, as potências ímpares de F tem todas o mesmo caráter χ_0 e as potências pares de F têm também todas o mesmo caráter χ_0.

Basta agora juntar as últimas duas proposições para concluir o resultado enunciado anteriormente, o Teorema do Género Principal.

Teorema 3.92 (Teorema do Género Principal)
Seja F uma forma quadrática binária. Então, podemos particionar as potências de F por dois géneros: As potências ímpares de F pertencerão ao género de F e as potências pares pertencerão ao género de F^2.

Chegámos ao fim de toda a teoria necessária e imprescindível para se entender os métodos de Gauss para gerar resíduos quadráticos[5].

[5]Esta parte foi bastante densa, felicitamos o leitor por aqui ter chegado.

Capítulo 4

Busca de resíduos quadráticos: Segunda Parte

Seja N um número inteiro do qual queremos encontrar a fatorização em primos. Na primeira parte deste método, no capítulo 2, estudámos como obter uma representação especifica de $\pm kN$ por uma forma quadrática[1] $F(x,y) = ax^2+cy^2$. Esta técnica requeria alguma destreza de cálculo, mas também podiamos calcular uma das raízes quadradas dos resíduos quadráticos encontrados (ver exemplo 2.15). A segunda parte do método envolve conhecer as características das formas quadráticas binárias mais a fundo, daí só ser apresentada após desenvolvermos alguma teoria sobre estes objetos. Este capítulo completa a exposição do artigo 332 de DA. Nas duas técnicas seguintes, consideramos $\pm kN$ como um determinante de formas quadráticas binárias.

4.1 Procedimento comum

Sejam duas formas quadráticas binárias $F = (a_0, b_0, c_0)$ e $G = (a_1, b_1, c_1)$ com o mesmo determinante $\pm kN = b_0^2 - a_0c_0 = b_1^2 - a_1c_1$ no mesmo género e suponhamos que temos α um número característico de F. Pela observação 3.73, como F e G estão no mesmo género, têm de ter os mesmos números característicos. Por isso, pelas propriedades dos números característicos, αa_0, αc_0, αa_1, αc_1 são resíduos quadráticos módulo kN.

Como o produto de resíduos quadráticos é um resíduo quadrático, temos que os números $\alpha^2 a_0c_0$, $\alpha^2 a_0a_1$, $\alpha^2 a_0c_1$, $\alpha^2 c_0a_1$, $\alpha^2 c_0c_1$ e $\alpha^2 a_1c_1$ são resíduos quadráticos módulo kN, e pelo teorema 1.43, módulo N. Podemos aplicar o lema da Eliminação do Quadrado, o lema 2.1, devido à definição de número característico, e eliminar o termo quadrado. No final, sobram a_0c_0, a_0a_1, a_0c_1, c_0a_1, c_0c_1 e a_1c_1 como resíduos quadráticos módulo N.

[1] É de notar que a representação $ax^2 + c$ é um caso particular, já que $ax^2 + c = ax^2 + c \cdot 1^2 = f(x,1)$

4.2 Formas quadráticas num mesmo período

Pegando nas observações anteriores, consideremos $F_0 = (a_0, b_0, a_1)$ uma forma reduzida de determinante positivo kN. Para esta forma, podemos calcular o seu período

$$F_0 = (a_0, b_0, a_1),\ F_1 = (a_1, b_1, a_2),\ F_2 = (a_2, b_2, a_3),\ F_3 = (a_3, b_3, a_4),\ \ldots\ ,\ F_m = (a_m, b_m, a_0).$$

Cada uma destas formas será propriamente equivalente a F_0, pelo que constarão da mesma classe de equivalência e assim pertencerão ao mesmo género. Por conseguinte, os números a_0a_1, a_0a_2, $\ldots a_0a_m$ serão resíduos quadráticos módulo kN, e portanto módulo N.

No capítulo anterior, na subsubsecção 3.2.1, vimos como calcular formas quadráticas reduzidas para um determinante D dado. Podemos procurar formas reduzidas com os menores coeficientes iniciais, e assim obter resíduos quadráticos de baixo valor absoluto. Um bom ponto de partida para se ter uma forma nestas condições é considerar a forma quadrática binária $F = (1, d_0, -k_0)$, sendo $d_0 = \lfloor \sqrt{kN} \rfloor$ e $\det(F) = kN = d_0^2 + k_0$. Esta é a fórmula (2.2). De seguida, após encontradas algumas formas quadráticas reduzidas, podemos usar o algoritmo 3.2 para calcular várias formas no período destas formas e obter resíduos quadráticos de N.

No artigo 187 do DA, Gauss enuncia um algoritmo de mais simples execução para encontrar os coeficientes a_i e b_i, o qual pode ser deduzido através do original. Esta versão é útil se o determinante D tiver uma ordem de grandeza elevada, e depende apenas de uma relação entre os coeficientes. Suponhamos que temos 2 formas quadráticas binárias $F_i = (a_i, b_i, a_{i+1})$ e $F_{i+1} = (a_{i+1}, b_{i+1}, a_{i+2})$ no mesmo período. Como têm de ter o mesmo determinante, vem que

$$D = b_i^2 - a_i a_{i+1} = b_{i+1}^2 - a_{i+1}a_{i+2}.$$

Através de alguns cálculos, obtemos a seguinte relação[2]:

$$a_{i+2} = \frac{b_{i+1} + b_i}{a_{i+1}} \cdot (b_{i+1} - b_i) + a_i.$$

Usando esta relação, temos uma técnica mais simples para obter formas distintas no mesmo período e assim obter resíduos quadráticos de kN.

Observação 4.1 (Recomendação de cálculo)
Caso a seja um resíduo quadrático módulo kN e $\mathrm{mdc}(a, N) = 1$, é possível que a seja o coeficiente inicial de uma forma quadrática reduzida. Após calcular uma forma F_0 nestas condições, podemos obter o seu período $(F_0, F_1, \ldots, F_m)$. Como exemplo não exaustivo, sabemos que aa_1, aa_2, $\ldots$, aa_m serão resíduos quadráticos módulo kN. No entanto, como a é resíduo quadrático, pelo lema da Eliminação do Quadrado, podemos simplificar estes resíduos para a_1, a_2, $\ldots$, a_m.

Exemplo 4.2
Para $N = 997331$, vem que $d_0 = 998$ e $997331 = 998^2 + 1327$. Donde, $F = (1, 998, -1327)$. Na tabela seguinte, reunimos parte do seu período e alguns resíduos quadráticos.

[2] É importante relembrar que a_{i+1} divide $b_{i+1} + b_i$.

Período de F	Resíduos	Fatorização	Período de F	Resíduos	Fatorização
$(1, 998, -1327)$	1	1	$(37, 987, -626)$	37	37
$(-1327, 329, 670)$	-1327	-1327	$(-626, 891, 325)$	-626	$-2 \cdot 313$
$(670, 341, -1315)$	670	$2 \cdot 5 \cdot 67$	$(325, 734, -1411)$	325	$13 \cdot 5^2$
$(-1315, 974, 37)$	-1315	$-5 \cdot 263$	$(-1411, 677, 382)$	-1411	$-17 \cdot 83$

Tabela 4.1: Parte do período da forma quadrática binária $F = (1, 998, -1327)$

Podemos[3] *considerar os resíduos quadráticos* $2 \cdot 5 \cdot 67$, 37, 13, $-17 \cdot 83$.

4.3 Potências de Formas Quadráticas

Vimos no final do último capítulo como se comportam as potências de uma forma quadrática quanto à sua divisão pelos géneros possíveis. Nesta parte do método, Gauss aconselha a que tomemos F uma forma quadrática binária de determinante negativo[4] kN. Caso consideremos as potências ímpares de F, temos que estas pertencerão todas ao mesmo género de F e, caso consideremos todas as potências pares de F, estas pertencerão todas ao género de F^2, o género principal, pelo teorema 3.92. Ao estarem no mesmo género, o produto dos coeficientes extremos de qualquer par de potências considerado será um resíduo quadrático módulo kN.

Observação 4.3 (Sobre as Potências Pares)
Será de extrema utilidade que as potências pares de F pertençam ao género principal, pois isto significa todo o número inteiro por si representado será resíduo quadrático módulo kN, em particular os coeficientes extremos.

No entanto, a composição por meios das formas unidas de Dirichlet é mais simples para descrever a operação do grupo criado por Gauss, mas não é útil para computação.

Observação 4.4 (Observação do mestrando)
Quanto à segunda potência de $F = (3, 1, 332444)$, o cálculo intermédio envolveu um coeficiente terminal c aproximadamente igual a 36.000.000. O processo de composição de Dirichlet é mais simples de ser explicado, mas os cálculos não são mais simples para serem executados à mão.

Para ajudar aos cálculos, transcrevemos um algoritmo de composição que se deve a Daniel Shanks, pensado para ser implementado maquinalmente, para formas quadráticas de determinante negativo. O leitor interessado poderá encontrar mais detalhes sobre o mesmo em ([Coh96], p. 247). No entanto, é preciso salientar que a definição de formas quadráticas deste livro é diferente da de Gauss, pelo que foi necessário fazer ajustes.
A ordem de magnitude dos cálculos é suficientemente baixa para poder ser executada por um ser humano, por muitos passos intermédios que acarrete. Omitiremos a sua demonstração, pois o algoritmo é fornecido apenas para ajudar o leitor a efetuar os mesmos cálculos que Gauss. Findo isto, podemos encontrar mais resíduos quadráticos dos múltiplos de 997331 e depois passaremos a uma possível implementação de raiz do algoritmo de Gauss para fatorizar inteiros.

[3] Podemos considerar muitos mais resíduos quadráticos, estes são os mais úteis para os nossos cálculos.
[4] Estamos a assumir que $k < 0$.

Algoritmo de Composição de Shanks

Seja $F_0 = (a_0, b_0, c_0)$ e $F_1 = (a_1, b_1, c_1)$ duas formas quadráticas binárias com o mesmo determinante D negativo. Vamos calcular $F_0 \odot F_1$ com as formas por esta ordem. Para estabelecer notação, a afirmação "$a \rightsquigarrow b$" significa que atribuimos à variável a o valor b.

1. Caso $a_0 > a_1$, trocamos a ordem e reiniciamos o cálculo com $F_1 \odot F_0$. De seguida, estabelecemos $s \rightsquigarrow b_0 + b_1$ e $n \rightsquigarrow 2b_1 - s$
2. (Primeiro Passo Euclidiano)
   - Caso $a_0 \mid a_1$, atribuimos $y_1 \rightsquigarrow 0$ e $d \rightsquigarrow a_0$ e passamos ao próximo passo.
   - Caso contrário, calculamos $d = \text{mdc}(a_0, a_1)$, e calculamos (u, v, d) tal que $ua_1 + va_0 = d$ e acabamos o passo com $y_1 \rightsquigarrow u$.
3. (Segundo Passo Euclidiano)
   - Caso $d \mid s$, estabelecemos $y_2 \rightsquigarrow -1$, $x_2 \rightsquigarrow 0$ e $d_1 \rightsquigarrow d$ e passamos ao próximo passo.
   - Caso contrário, calculamos $d_1 = \text{mdc}(s, d)$, e calculamos (α, β, d_1) tal que $\alpha s + \beta d = d_1$ e atribuimos $x_2 \rightsquigarrow \alpha$, $y_2 \rightsquigarrow -\beta$.
4. (Composição)
   - Calculamos $v_1 = \frac{a_0}{d_1}$, $v_2 = \frac{a_1}{d_1}$, $r \equiv y_1 y_2 n - x_2 c_1 \pmod{v_1}$.
   - De seguida, vêm os coeficientes $b_2 \rightsquigarrow 2b_1 + 2v_2 r$, $a_2 \rightsquigarrow v_1 v_2$, $c_2 \rightsquigarrow \frac{b_2^2 - 4D}{4a_2}$.
   - Neste ponto, temos uma forma $F_2 = (a_2, 2b_2, c_2)$.
5. Para obter uma resposta final, dividimos o coeficiente médio por 2 e obtemos a forma $F_2 = (a_2, b_2, c_2)$. De seguida, avaliamos se F_2 é uma forma reduzida. Caso seja reduzida, esta é a forma composta. Caso contrário, aplicamos o algoritmo de redução 3.1.

Tabela 4.2: Algoritmo de Shanks para a composição de formas quadráticas binárias com determinante negativo

Exemplo 4.5

Consideremos a forma $F = (3, 1, 332444)$ de determinante $D = -997331$. Podemos calcular algumas das suas potências usando os métodos de Dirichlet ou o algoritmo de Shanks. Após termos todas as potências em forma reduzida e representá-las como Gauss, podemos reuni-las numa tabela.

Potência	Forma Reduzida	Potência	Forma Reduzida
F^1	$(3, 1, 332444)$	F^6	$(729, -209, 1428)$
F^2	$(9, -2, 110815)$	F^7	$(476, 209, 2187)$
F^3	$(27, 7, 36940)$	F^8	$(1027, 342, 1085)$
F^4	$(81, 34, 12327)$	F^9	$(932, -437, 1275)$
F^5	$(243, 34, 4109)$	F^{10}	$(425, 12, 2347)$

Tabela 4.3: As primeiras 10 potências da forma quadrática binária $F = (3, 1, 332444)$

Analisando os coeficientes extremos das potências pares de F, obtemos logo os resíduos quadráticos seguintes a partir dos coeficientes finais: $110815 = 5 \cdot 37 \cdot 599$, $12327 = 3 \cdot 7 \cdot 587$, $1428 = 3 \cdot 7 \cdot 17 \cdot 2^2$, $1085 = 5 \cdot 7 \cdot 31$. *A partir do coeficiente inicial de* F^8 *também obtemos o resíduo* $1027 = 13 \cdot 79$.

Considerando as potências ímpares F^1 *e* F^9*, podemos multiplicar o coeficiente inicial de* F^1 *pelo coeficiente terminal de* F^9*, pelo que obtemos o resíduo quadrático,* $3 \cdot 1275 = 3^2 \cdot 5^2 \cdot 17$. *Como* $\text{mdc}(15, 997331) = 1$*, então podemos usar o lema da Eliminação do Quadrado e considerar apenas* 17 *como resíduo quadrático.*

Finalmente, multiplicando os resíduos quadráticos 17 *e* 1428*, obtemos o resíduo quadrático* $24276 = 17^2 \cdot 3 \cdot 7$. *Pelo Lema da Eliminação do Quadrado, podemos simplificar este resíduo para considerar o resíduo mais simples* $21 = 3 \cdot 7$.

4.3.1 Resíduos quadráticos finais

Como uma última tentativa de obter mais resíduos quadráticos de 997331, podemos juntar as duas técnicas vistas neste capítulo. Sabemos que 17 é resíduo quadrático de 997331, logo, tendo em mente a observação 4.1, consideremos a forma quadrática reduzida $(17, 989, -1130)$ de determinante 997331. Calculando o período desta forma, obtemos a sucessão de formas:

$$(17, 989, -1130), \quad (-1130, 141, 865), \quad (865, 724, -547), \quad (-547, 370, 1573),$$
$$(1573, -370, -547), \quad (-547, 370, 1573), \quad (1573, -370, -547), \quad (-547, 917, 286).$$

Desta sucessão, ao multiplicarmos os coeficientes iniciais da primeira e quinta forma, obtemos que $17 \cdot 1573$ é resíduo quadrático, e portanto 1573 também o será. Como $1573 = 11^2 \cdot 13$ é resíduo quadrático, então 13 também o será, pelo Lema da Eliminação do Quadrado. Do mesmo modo, ao multiplicarmos o coeficiente inicial da primeira forma e o coeficiente terminal da oitava forma, $17 \cdot 286$ é resíduo quadrático e, por tal, 286 é resíduo quadrático. Ao sabermos que 13 é resíduo quadrático, como $286 = 2 \cdot 11 \cdot 13$, vem que $22 = 2 \cdot 11$ é resíduo quadrático, pelo Lema da Eliminação do Quadrado.

Usando estas últimas técnicas, pudemos calcular resíduos quadráticos bastante menores que o número a fatorizar que era o nosso objetivo. A partir do capítulo anterior, uma vez que $-2 \cdot 3 \cdot 17$ é resíduo quadrático[5], podemos conjugá-lo com o resíduo quadrático 17 para obter que -6 é resíduo quadrático de 997331.

Para encontrar a fatorização de 997331 poderiamos então considerar os resíduos quadráticos[6]

$$-6, 13, 17, 21, 22, 37.$$

No próximo capítulo, veremos como usar resíduos quadráticos para fatorizar números inteiros.

[5]Foi calculado no capítulo 2.

[6]No anexo A usamos estes resíduos quadráticos de forma a fatorizar 997331.

Capítulo 5

Crivo Gaussiano

O presente capítulo é o culminar de tudo o que vimos. No final do capítulo 6 do *Disquisitiones Arithmeticae*, após desenvolver um trabalho extenso sobre formas quadráticas binárias no capítulo precedente, Gauss expõe uma sua aplicação na secção entitulada "Dois métodos para distinguir números compostos de números primos e para determinar os seus fatores"[1] composta pelos artigos numerados entre 329 a 334 de DA. Deste modo, responde a uma declaração de Lambert de 1770:

> *"O que é preciso notar com respeito aos métodos de fatorização propostos até agora é que os primos demoram mais tempo, e não conseguem ser fatorizados. Isto é porque não há forma de conhecer de antemão se um número dado tem divisores ou não."* ([GSS07], p. 14).[2]

Após termos visto várias técnicas para encontrar resíduos quadráticos de N nos capítulos anteriores, o nosso objetivo será usar estes resíduos para obter a fatorização em primos de N. No artigo 329, antes da procura de qualquer resíduo quadrático, de modo a não usar técnicas demasiado avançadas à partida, Gauss sugere fazer a divisão por alguns primos pequenos entre 2 e 19 ou um pouco mais além. Não nos é dada nenhuma razão para este limite superior. Como objeto do seu estudo, é-nos apresentado o número 314159265 (o qual podemos reconhecer como os primeiros algarismos da expansão decimal de pi). Fazendo algumas divisões por primos pequenos, temos uma primeira fatorização em primos deste número.

$$314159265 = 3^2 \cdot 5 \cdot 7 \cdot 997331$$

Agora, o problema de fatorizar o primeiro número em primos reduz-se ao problema de se fatorizar 997331 em primos, o qual é de uma ordem de magnitude menor. No entanto, antes de progredir, é necessário ter em consideração que existem critérios de divisibilidade de aplicação simples que podem simplificar os cálculos sem ser necessária a divisão pelo número em questão. Recolhemos uns quantos no anexo B, do qual aconselhamos a leitura.

[1] No original: "Duae methodi, numeros compositos a primis dignoscendi, illorumque factores inuestigandi"

[2] No original: "What one has to note with respect to all factorization methods proposed so far, is that primes take longest, yet cannot be factored. This is because there is no way of knowing beforehand whether a given number has any divisors or not."

5.1 Exclusão de candidatos

Poder-se-ia dividir o número pretendido por todos os números primos que lhe são inferiores, mas isso seria excessivo pelo resultado que se apresenta de seguida.

Teorema 5.1 (Primos abaixo da raiz)
Seja $N \in \mathbb{N}_4$ composto. Então, existe um primo p_i divisor de N tal que $p_i \leqslant \sqrt{N}$.

Demonstração. Sejam $b, c \in \mathbb{N}_2$, $N \in \mathbb{N}_4$ t.q. $bc = N$. Sem perda de generalidade, assuma-se $b \leqslant c$. Donde, $b^2 \leqslant bc = N$. Ou seja, $b \leqslant \sqrt{N}$. Caso b seja primo, a demonstração fica concluída. Caso contrário, tome-se p_1 divisor primo de b. Pelas propriedades da divisão, vem que $p_1 \leqslant b \leqslant \sqrt{N}$ e tem-se o pretendido.

Q.E.D.

Observação 5.2
Gauss salienta que pode haver um fator primo q tal que $\sqrt{N} < q$. Repare-se que $14 = 2 \cdot 7$, mas $\sqrt{14} < 7$. No entanto, um fator primo nestas circunstâncias tem de ser único.

Demonstração. Queremos provar a unicidade do fator primo. Argumentemos por contradição. Sejam $b, c \in \mathbb{N}_2$, $d \in \mathbb{N}_1$, $N \in \mathbb{N}_4$, e $\varepsilon, \delta > 0$. Suponhamos que $N = bcd$, com $b = \sqrt{N} + \varepsilon$ e $c = \sqrt{N} + \delta$ primos. Então,

$$N = bcd = (\sqrt{N} + \varepsilon) \cdot (\sqrt{N} + \delta) \cdot d = (N + \varepsilon\delta + (\varepsilon + \delta)\sqrt{N}) \cdot d > N, \tag{5.1}$$

o que é absurdo.

Q.E.D.

O artigo 330 da obra *Disquisitiones Arithmeticae* abre com uma referência a um teorema importante, o teorema 1.43 (Artigo 105, DA), do qual podemos deduzir o corolário seguinte.

Corolário 5.3 (Corolário da Exclusão)
Seja a resíduo quadrático módulo N, e seja q um número primo tal que a é não-resíduo quadrático módulo q. Então q não divide N.

Demonstração. Vem diretamente do teorema citado. Para que a seja resíduo quadrático mod N, tem de ser resíduo quadrático mod d de qualquer divisor d de N. Se há um primo q tal que a é não-resíduo quadrático mod q, então q não pode ser um divisor de N. Q.E.D.

Este corolário será a base para encontrar a fatorização em primos de um número inteiro N. O objetivo é encontrar resíduos quadráticos para excluir candidatos a divisores de N, num processo semelhante ao crivo de Eratóstenes, pelo que chamámos *Crivo Gaussiano* a este método.

5.2 O processo de exclusão

Suponhamos que queremos fatorizar N em primos. Antes de tudo, será útil seguir os conselhos de Gauss e fazer uma primeira busca pelos primeiros primos, seja dividindo ou aplicando algum

critério de divisibilidade. De seguida, quando consideramos candidatos a divisores, pelo teorema 5.1 vem que é suficiente procurar divisores primos não-superiores à raiz quadrada de N.
Agora, é possível otimizar esta busca usando o corolário 5.3. O objetivo será encontrar resíduos quadráticos de N. Caso tenhamos r, um seu resíduo quadrático, é possível excluir — de entre os candidatos prévios — os primos dos quais r é um não-resíduo quadrático. Isto, por regra geral, costuma eliminar metade dos candidatos a primos.

Observação 5.4 (Justificação da taxa de exclusão)
Usamos o termo "regra geral", pois o próprio Gauss, ao explicar que se eliminam metade dos candidatos a divisores de N, não dá total certeza sobre tal. Apresenta-se, de seguida, o argumento que é usado no artigo 147, da obra estudada.
Seja q número primo da forma $4k+1$. Podemos aplicar a Lei da Reciprocidade Quadrática (teorema 1.24) para saber de que primos p é q um resíduo quadrático.

$$1 = \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Como q é da forma $4k+1$, ficamos com

$$1 = \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

Assim, p tem de ser congruente a um resíduo quadrático mod q. Donde, baseando-nos na observação 1.29, estes primos p estarão em progressões aritméticas da forma $qk+a$, sendo a resíduo quadrático módulo q. Na observação 1.7 expomos que o número de resíduos quadráticos módulo q será $\frac{q-1}{2}$. O que significa que q será resíduo quadrático de primos em $\frac{q-1}{2}$ progressões aritméticas das $q-1$ possíveis.

Suponhamos que encontramos r' um outro resíduo de N. Pode acontecer que rr' seja um número quadrado. Neste caso, rr' será resíduo quadrático de todo o primo p, e portanto, r e r' serão resíduos quadráticos para exatamente os mesmos primos. Neste caso, Gauss diz que r e r' não são *independentes*.

Observação 5.5
Caso rr' seja um número quadrado não-nulo, então será resíduo quadrático mod p, para qualquer p primo. Em particular, suponhamos que r também é resíduo quadrático mod p. Então, as próximas congruências serão possíveis:

$$x^2 \equiv rr' \pmod{p} \qquad \text{e} \qquad y^2 \equiv r \pmod{p}.$$

Deste modo, fazendo a substituição da segunda congruência na primeira congruência, vem:

$$x^2 \equiv y^2 r' \pmod{p}.$$

Assim a próxima congruência também será possível,

$$(xy^{-1})^2 \equiv r' \pmod{p}.$$

E assim, r' é resíduo quadrático de todos os primos dos quais r é resíduo e vice-versa.

Quando r, r' são independentes, então a regra geral continua a aplicar-se e, após a exclusão de candidatos por r, excluímos metade dos restantes candidatos a primos usando o resíduo r'. E assim sucessivamente para futuros resíduos r'', r''', etc.
No artigo 331, Gauss dá uns exemplos de como poderia funcionar esta exclusão em metade. Como já foi referido, pela observação 1.29, os primos para os quais um certo r será resíduo quadrático estão em progressões aritméticas da forma $rz + a$ ou $4rz + a$. Quando os resíduos são números muito pequenos, podemos basearmo-nos nestas formas lineares para fazer a exclusão pretendida. A título de exemplo, recuperemos o corolário 1.16.
Considerando $N \in \mathbb{N}$, suponhamos que -1 é resíduo quadrático de N. Como -1 é resíduo quadrático apenas dos primos da forma $4k + 1$, usando o corolário 5.3, excluímos todos os números primos candidatos a divisores da forma $4k + 3$. Igualmente, tendo 2 como resíduo quadrático, significa que excluímos todos os primos da forma $8k \pm 3$ uma vez que 2 só é resíduo quadrático dos primos da forma $8k \pm 1$. Pelas contas dos exemplos 1.27 e 1.28, vemos que ao ter 5 como resíduo quadrático de N excluímos todos os primos da forma $5k \pm 2$ e ao ter 3 como resíduo quadrático de N excluímos todos os primos da forma $12k \pm 5$. Estes métodos estão longe de ser eficientes e Gauss sugere a criação de um instrumento, o qual se detalha mais adiante.
Como últimas considerações, no artigo 330, Gauss afirma que o número de candidatos a divisores de N diminuirá rapidamente até que não sobre nenhum. Neste caso, N será primo. Também se pode dar o dar o caso de sobrarem tão poucos que a divisão por cada um deles pode ser efetuada sem grande dificuldade. Segundo Gauss, para números que não excedem 10^6, usualmente 6 ou 7 exclusões serão suficientes e para números que não excedem 10^9, o número de exclusões necessário sobe para 9 ou 10.

Observação 5.6 (Observação do mestrando)
Após dedicar várias tardes e noites à busca de resíduos apropriados, é preciso notar que são dificeis de encontrar — não só pelo aspeto teórico, mas também pelos meios disponíveis. O número de exclusões anterior pode ser o aconselhado por Gauss, mas pode ser demasiado custoso encontrar este número de resíduos quadráticos. Deter 3 resíduos apropriados foi suficiente para que o número de divisões pelos candidatos restantes fosse consideravelmente menor.

5.3 Instrumentos físicos

No artigo 331, Gauss sugere a criação de um instrumento físico semelhante a uma tabela para efetuar a filtragem, uma vez que a ordem de grandeza do resíduo quadrático r pode tornar inviável a exclusão por formas lineares $rz + a$ ou $4rz + a$.
Seja $N \in \mathbb{Z}$, o número inteiro que queremos fatorizar. Esta tabela ajudaria à implementação do processo a que chamámos Crivo Gaussiano, de forma a separar os divisores de N dos números que não o dividem. Para que este instrumento tenha a máxima utilidade, Gauss sugere que cada coluna seja independente, possa ser rearrumada e removível, citando o exemplo dos Ossos de Napier[3]. Seguindo esta recomendação, teremos assim um dispositivo constituido por um

[3]Instrumento de cálculo constituido por varetas verticais amovíveis.

conjunto de varetas verticais amovíveis.

Numa primeira fase, todas as varetas serão divididas em células por meio de linhas horizontais paralelas de alto a baixo. Uma vez que vamos alinhar estas varetas para efetuar o processo de crivagem, é necessário ter células com a mesma altura e em igual número em cada coluna.

A primeira vareta recebe o nome de VARETA DOS MÓDULOS, pois dela somente constam os módulos, isto é, os números primos que vamos testar como candidatos a divisores de N. Em cada célula há exatamente um número primo, ou seja, preenchemos a célula i com o número primo p_i. Como recomendação desta dissertação, aconselhamos a que a primeira célula não esteja preenchida, podendo optar por deixá-la em branco como fez Gauss, ou então desenhando um símbolo qualquer à escolha do leitor. As varetas seguintes constroem-se de forma semelhante. A primeira célula estará preenchida com um número inteiro r livre de quadrados, o qual pode ser positivo ou negativo. Precisaremos de ter varetas encabeçadas por r primo. No entanto, r também pode ser composto, ainda que não seja totamente necessário (ver observação 5.7). Como tal, indexamos cada vareta destas em ordem ao seu cabeçalho e referimo-nos à vareta v_r como a vareta que tem a primeira célula preenchida com r. De seguida, as células subsequentes de uma vareta arbitrária v_r podem ser ou deixadas em branco ou preenchidas. Preenchemos a i-ésima célula desta vareta, caso a congruência $x^2 \equiv r \pmod{p_i}$ seja possível.

Após termos todas as varetas preenchidas adequadamente, escolhemos as varetas v_r possíveis para as quais r é resíduo quadrático de N. De seguida, tomamos a coluna dos módulos e alinhamos as colunas v_r escolhidas com esta num renque de forma a que as células i de cada coluna v_r estejam na mesma linha.

O passo de exclusão far-se-á de seguida. Neste momento, procuramos os primos p_i na vareta dos módulos tais que as células i de cada vareta v_r estão preenchidas. Se a algum primo p_i lhe corresponde uma vareta v_r com um espaço vazio na célula i, esse primo deverá ser desconsiderado. Este passo de exclusão deve-se ao corolário 5.3. Na próxima secção veremos o culminar de tudo o que foi estudado, ao descobrir os fatores primos um número inteiro.

Observação 5.7 (Observação do mestrando)
Podemos usar múltiplas varetas para cumprir o papel de um número composto[a]. Seja R resíduo de N t.q. $R = ab$ com $a, b \in \mathbb{Z}$ e p um número primo. Neste caso, R será resíduo quadrático módulo p se, ou a e b são resíduos quadráticos módulo p, ou a e b são não-resíduos quadráticos módulo p. Assim, para testar se R é resíduo quadrático módulo p, basta analisar as células das varetas v_a e v_b na linha referente a p. Se estiverem ambas preenchidas ou ambas não-preenchidas, R será resíduo quadrático módulo p. Caso contrário, R é não-resíduo quadrático módulo p. Desaconselhamos usar três ou mais varetas, devido ao número de combinações possíveis.

[a]No Anexo A (p.84) dispomos um exemplo deste caso.

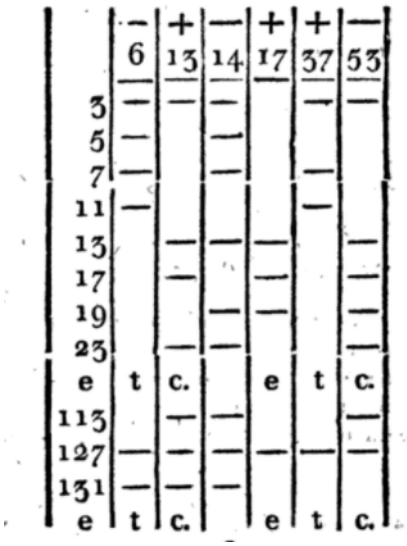

Figura 5.1: A fatorização de 997331 presente em Disquisitiones Arithmeticae. Só está tracejada totalmente a linha do 127, logo é um candidato a divisor de 997331. Realmente, 997331 = 127·7853.

5.4 Uma primeira técnica

Após o exposto nas páginas anteriores, podemos reconstruir uma técnica para fatorizar um número em primos, usando as ideias de Gauss. É muito provável que Gauss também tivesse uma técnica para uso próprio, como o parece indicar uma nota de rodapé no artigo 331 de DA.

> *"O autor construiu para uso próprio uma grande parte da tabela aqui descrita e tê-la-ia publicado com muito gosto se houvesse interessados em número suficiente para justificar esse esforço. Se houver algum devoto da aritmética que compreenda os princípios envolvidos e deseje construir uma tabela como esta por si, o autor terá grande prazer em comunicar por via de carta todos os procedimentos e artifícios que usou."* ([Gau01], p.582)[4]

Para adiantar trabalho, usaremos o número 21037, pois já foi trabalhado em páginas anteriores.

Divisão por primos

Ao acaso, consideremos um número inteiro N, e seja $d \in \mathbb{N}_1$. Pelo Algoritmo da Divisão, podemos dividir N por d e sabemos que o resto nesta divisão será um entre d restos possíveis. Dizemos que N é múltiplo de d se este resto for 0. Logo, o problema de calcular a probabilidade de ser múltiplo de d, reduz-se ao problema de calcular a probabilidade de ter resto 0 entre d restos possíveis.

A probabilidade de ser divisível por p será $\frac{1}{p}$ e a probabilidade de não ser múltiplo de p é $\left(1-\frac{1}{p}\right)$. Tomando primos $p, q, r, \ldots$, a probabilidade de não ser divisível por nenhum deles será

$$\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots$$

Portanto, tendo um número ao acaso, a probabilidade de não termos um múltiplo de $3, 5, 7, 11, 13, 17, 19$ será

$$\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)\left(1-\frac{1}{17}\right)\left(1-\frac{1}{19}\right) \approx 0.3420480\ldots$$

Apenas 34% dos elementos de $\mathbb{Z}$ não terá estes números como fatores e para números inferiores a 529, teremos feito todas as divisões necessárias. Isto deve-se a termos $529 = 23^2$ e o teorema 5.1. De forma semelhante, podemos calcular a percentagem dos números sem fatores menores que 100 (12%), menores que 139 (11%), e menores que 1000 (8%). Este cálculo foi automatizado e está presente em D.2.3. Tomando $N = 21037$, após algumas divisões, obtemos:

$$\begin{aligned} 21037 &= 2 \cdot 10518 + 1 = 3 \cdot 7012 + 1 \\ &= 5 \cdot 4207 + 2 = 7 \cdot 3005 + 2 \\ &= 11 \cdot 1912 + 5 = 13 \cdot 1618 + 3 \\ &= 17 \cdot 1237 + 8 = 19 \cdot 1107 + 4. \end{aligned}$$

[4] No original: "Auctor apparatum satis amplum tabulae hic descriptae, quem ad vsum suum construendum curauit, publici iuris lubenter faceret, si paucitas eorum, quibus vsui esse potest, sumtibus talis incepti sustentandis sufficeret. Si quis interea arithmeticae amator, principiis probe penetratis, proprio marte talem tabulam sibi condere optat, auctor magnae voluptati sibi ducet, omnia cum eo emolumenta ac artificia per literas communicare"

Símbolos de Jacobi

Este instrumento é posterior à publicação do DA. No entanto, descende diretamente das ideias por ele veiculadas, pelo que consideramos o seu uso não ser demasiado anacrónico.

Observação 5.8
Ao termos um instrumento físico, estaremos limitados às tabelas que dele constam. No entanto, sabemos que o símbolo de Jacobi não devolve falsos negativos, pela proposição 1.45. Assim, podemos excluir colunas do instrumento a considerar consoante os valores que obtivermos, o que pode ser útil para decidir que coeficientes iniciais usamos para a decomposição estudada[5]:

$$ax^2 + cy^2 = kN. \tag{5.2}$$

Assumindo que $\text{mdc}(ax^2, cy^2) = 1$, sabemos que $-ac$ será resíduo quadrático de N. Caso a fosse resíduo quadrático de N, poderiamos multiplicá-lo por $-ac$ e concluir que $-c$ é resíduo quadrático de N, pelo lema 2.1 (ver exemplo 2.2). Ao termos que a é não-resíduo quadrático de N, é impossível fazer simplificações como estas.

Pelas proposições 1.38 e 1.39, pela observação 1.40 e pelo teorema 1.41, temos maneiras simples de calcular símbolos de Jacobi com o objetivo de excluir candidatos a resíduos quadráticos de N. Para usarmos a observação 1.40, convém fazer as divisões seguintes:

$$21037 = 4 \cdot 5259 + 1 = 8 \cdot 2629 + 5.$$

- Como $21037 \equiv 1 \pmod 4$, -1 pode ser resíduo quadrático mod 21037.
- Como $21037 \equiv 5 \pmod 8$, 2 é não-resíduo quadrático mod 21037.

Podemos usar as anteriores divisões de 21037, a Lei da Reciprocidade Quadrática e a proposição 1.38 para calcular símbolos de Jacobi:

- $\left(\frac{3}{21037}\right) = \left(\frac{7}{21037}\right) = \left(\frac{11}{21037}\right) = \left(\frac{13}{21037}\right) = \left(\frac{17}{21037}\right) = \left(\frac{19}{21037}\right) = 1.$
- $\left(\frac{5}{21037}\right) = -1$ — Não-resíduo quadrático.

Desta forma, já excluímos $2, 5$ como possíveis resíduos quadráticos.

Decomposições $ax^2 + cy^2 = kN$ e $ax^2 + cn = kN$

Nesta parte do método, a ideia é decompôr o número dando valores a a, a y e a k, tendo em atenção tudo o que já foi dito. Para facilidade de cálculo, parte das contas desta secção já foram trabalhadas anteriormente na secção 2.2. É aconselhável começar pelas equações $ax^2 + cn = N$, sendo a um dos números primos pelos quais efetuámos as primeiras divisões, pois já temos vários dados que nos facilitam a tarefa. De seguida, caso exista, basta procurar o próximo valor de x que satisfaça $ax^2 + cy^2 = kN$. Para o caso de 21037, escolhemos 3 que nos permitem ter resíduos de uma ordem de grandeza muito reduzida e apresentamo-las na tabela seguinte.

[5] O mesmo se aplica para as decomposições $ax^2 + c$ e $ax^2 + cn$.

Na coluna *Resíduos*, temos os resíduos -1 e -3, e $3 \cdot 7$. Multiplicando os resíduos -1 e -3, obtemos que 3 é resíduo quadrático mod 21037. Do mesmo modo, para forçar a existência de um número quadrado, podemos multiplicar 3 com o resíduo $3 \cdot 7$ e temos que $3^2 \cdot 7$ é resíduo quadrático. Aplicando o Lema da Eliminação do Quadrado, podemos concluir que 7 é resíduo quadrático. Sobram os resíduos quadráticos $-1, 3, 7$. Este género de simplificações é particularmente útil de modo a ter os melhores resíduos quadráticos a usar.

Decomposição	Resíduos
$145^2 + 3 \cdot 2^2 = 21037$	-3
$205^2 + 7^2 = 2 \cdot 21037$	-1
$3 \cdot 188^2 - 7 \cdot 11^2 = 5 \cdot 21037$	$3 \cdot 7$

Tabela 5.1: Algumas decomposições e resíduos quadráticos apropriados de 21037

Período de formas quadráticas

Usando as recomendações anteriores, podemos considerar formas quadráticas reduzidas de determinante 21037 e calcular os seus períodos. Começando com a forma reduzida $F = (1, 145, -12)$, que calculámos anteriormente, podemos calcular o seu período e representá-lo na seguinte tabela.

Período de F	Resíduos Quadráticos	Período de F	Resíduos Quadráticos
$F_0 = (1, 145, -12)$	1	$F_7 = (-27, 137, 84)$	-27
$F_1 = (-12, 143, 49)$	-12	$F_8 = (84, 115, -93)$	84
$F_2 = (49, 102, -217)$	49	$F_9 = (-93, 71, 172)$	-93
$F_3 = (-217, 115, 36)$	-217	$F_{10} = (172, 101, -63)$	172
$F_4 = (36, 137, -63)$	36	$F_{11} = (-63, 88, 211)$	-63
$F_5 = (-63, 115, 124)$	-63	$F_{12} = (211, 123, -28)$	211
$F_6 = (124, 133, -27)$	124	$F_{13} = (-28, 129, 157)$	-28

Tabela 5.2: Uma parte do período da forma quadrática binária $F = (1, 145, -12)$

Para esta forma quadrática, esta técnica revela ser bastante frutífera, uma vez que obtemos resíduos quadráticos bastante úteis apenas com o cálculo de algumas formas.

- A partir do coeficiente inicial de F_1 obtemos o resíduo -12, o qual fornece o resíduo -3.
- A partir do coeficiente inicial de F_5, obtemos o resíduo -63 o qual fornece o resíduo -7.
- A partir do coeficiente inicial de F_6, obtemos o resíduo 124 o qual fornece o resíduo a 31. Este último também poderia ser encontrado através do coeficiente inicial de F_3 pois -7 é resíduo quadrático.

Embora não tenhamos encontrado muitos mais resíduos quadráticos novos, requereram menos contas para serem encontrados.

Composição de formas quadráticas

Usando as técnicas do capítulo 3, também podemos considerar uma forma quadrática reduzida de determinante -21037 como $G = (13, 6, 1621)$ e calcular as suas potências, as quais transcrevemos na tabela abaixo.

Potências de F	Forma	Potências de F	Forma
F^1	$(13, 6, 1621)$	F^6	$(118, -47, 197)$
F^2	$(137, 46, 169)$	F^7	$(17, -3, 1238)$
F^3	$(41, -18, 521)$	F^8	$(97, 20, 221)$
F^4	$(46, 13, 461)$	F^9	$(53, -2, 397)$
F^5	$(37, -4, 569)$	F^{10}	$(134, -1, 157)$

Tabela 5.3: Potências da forma quadrática binária $F = (13, 6, 1621)$

Potências pares

Após estes cálculos, podemos começar por analisar as potências pares. Vimos que todos os números que se representam por estas potências serão resíduos quadráticos de 21037.

1. A partir da forma F^2, analisamos o coeficiente inicial e temos que 137 é resíduo quadrático. No entanto, por tentativa e erro, calculando $F_2(9, 5) = 19462 \equiv -1575 \pmod{21037}$. Após alguns cálculos, como $-1575 = 5^2 \cdot 3^2 \cdot (-7)$, concluímos que -7 é resíduo quadrático.

2. A partir da forma F^4, pelo coeficiente inicial, deduzimos que 46 é resíduo quadrático.

3. A partir da forma F^8, pelo coeficiente inicial, deduzimos que 97 é resíduo quadrático, mas também pelo coeficiente terminal, temos que 221 é resíduo quadrático. Também podemos calcular, por tentativa e erro, $F^8(8, 8) = 22912 \equiv 1875 \pmod{21037}$. Deste modo, $1875 = 3 \cdot 25^2$. Assim, 3 também é resíduo quadrático de 21037.

Potências ímpares

Uma vez que as formas quadráticas F^1 e F^7 estão no mesmo género, podemos multiplicar os coeficientes iniciais e temos que $13 \cdot 17$ é resíduo quadrático. No entanto, este resíduo já tinha sido encontrado pois $13 \cdot 17 = 221$.

Para a nossa exclusão de candidatos, os resíduos quadráticos mais proveitosos são -1, 3 e 7, pelo que serão os usados no processo. Sabemos que $\sqrt{21037} \approx 145,04$, logo, só precisamos de procurar candidatos a divisores primos de 21037 até 146.
Como vemos na tabela 5.4, após usarmos 3 resíduos quadráticos, notamos que sobram 37 e 109 como candidatos a divisores de 21037. Após dividir 21037 por 37 e por 109, notamos que 109 divide[6] 21037, pelo que concluimos[7] que $21037 = 109 \cdot 193$.

p	-1	3	7
3		■	■
5	■		
7			■
...	...	...	...
37	■	■	■
...	...	...	...
109	■	■	■
...	...	...	...

Tabela 5.4: Crivo Gaussiano para 21037

[6] Ao continuar a calcular as potências da forma quadrática $F = (13, 6, 1621)$, mostramos que $F^{12} = (109, 0, 193)$. Este cálculo significa que $21037 = 109 \cdot 193$, ou seja, também temos uma fatorização de 21037.

[7] Uma visualização alternativa encontra-se no anexo A (p.84).

Conclusão

Foi uma longa e agradável viagem para chegarmos até aqui, mas esta dissertação de mestrado chegou ao fim. Ao longo deste texto, expusemos o problema da "fatorização de números inteiros" e uma das primeiras abordagens à sua resolução. É impressionante que Gauss tenha conseguido criar um método tão sofisticado a partir de um teorema tão simples como o teorema 1.43 e o seu corolário 1.44.

No entanto, ainda que tenha sido pioneiro na sua época, é tambem bastante claro que este método está algo desatualizado tendo em conta os desenvolvimentos atuais das tecnologias de computação e da própria Teoria dos Números. No tempo de matemáticos como Fermat, Euler e Gauss, as preocupações que levaram ao nascimento da Teoria dos Números não passavam de meros desafios intelectuais. Hoje em dia, a segurança dos nossos dados e comunicações delas depende. De tal forma que, com a tecnologia apropriada, em segundos podemos calcular a fatorização em primos de certos números com uma elevada ordem de grandeza[8], ou calcular números primos com milhares de dígitos, etc.

Porém, conhecer o Passado pode ser de grande ajuda para entender o Presente. Parte das ideias expostas (resíduos quadráticos e formas de os gerar, a congruência de quadrados, etc.) continuam a ser parte integrante de alguns dos algoritmos de fatorização de inteiros atuais como o Crivo Quadrático de Pomerance, como se pode consultar em [AN17].

À data da elaboração desta dissertação, os resíduos quadráticos continuam a ser um objeto imprevísivel. O capítulo 1 serviu exatamente para mostrar isso: se estivermos a analisar o conjunto dos resíduos quadráticos de um número inteiro N, há menos estrutura se N for composto, do que se N fosse primo. É fácil calcular todos os resíduos quadráticos de N, simplesmente atribuindo valores à função $f(x) = x^2$ e fazer a congruência módulo N; e, caso estejamos a considerar um número primo p, é-nos simples discernir com certeza se um número inteiro a é resíduo quadrático módulo p ou não. Mas, basta estudarmos os resíduos quadráticos de um número composto e deparamo-nos com obstáculos como os falsos positivos e a sua própria ordem de magnitude. O melhor que conseguimos fazer é excluir logo os não-resíduos quadráticos.

Pelo que vimos na secção 2.2, se conhecermos todos os resíduos quadráticos de um número N, conseguimos chegar à sua fatorização em primos (ver 'fatorização de Fermat'). No entanto, se soubermos qual é a fatorização em primos de N, conseguimos eliminar os falsos positivos

[8]Por exemplo, em páginas *web* como [Alp21] ou [Res21]

quando procuramos averiguar se a é resíduo quadrático módulo N ou não. Por conseguinte, o problema de distinguir entre os resíduos quadráticos e os não-resíduos quadráticos de N está intimamente relacionado com o problema da fatorização em primos. Uma solução para um dos problemas oferece uma solução para o outro.

O problema da fatorização em primos tem especial relevância nos dias de hoje, sobretudo devido à Criptografia. O criptosistema RSA é um dos criptosistemas em uso corrente nos dias de hoje, do qual depende a segurança na troca de dados e mensagens na Internet ([Bla14]), por exemplo, na autenticação de transações bancárias. O uso corrente deste criptosistema deve-se à grande dificuldade de fatorizar números inteiros; assim sendo, caso tenhamos um algoritmo eficiente para o fazer, podemos comprometer a segurança de populações inteiras. Os trabalhos de Gauss, embora sejam de conhecimento geral (uma vez que são a base da Teoria dos Números), reforçam a ligação entre um problema tão dantesco como a fatorização em primos e algo tão simples como formas quadráticas.

Por agora, citando Andrew Wiles aquando da demonstração do Último Teorema de Fermat, "Acho que vou parar por aqui."[9]

[9]No original: "I think I'll stop here."

Bibliografia

[Alp21] Darío Alpern. *Calculadora de factorización de numeros enteros*. Sitio Web de Darío Alpern, 2021. URL: https://www.alpertron.com.ar/ECMC.HTM.

[AN17] Paulo J. Almeida e Diego Napp. *Criptografia e Segurança*. Porto: Porto: Publindústria, 2017.

[BK09] Mark Beintema e Azar Khosravani. «The Origins of the Genus Concept in Quadratic Forms». English. Em: *The Montana Mathematics Enthusiast* 6.1-2 (jan. de 2009), pp. 137–150. URL: https://scholarworks.umt.edu/tme/vol6/iss1/13/.

[Bla14] Stephanie Blanda. *RSA Encryption – Keeping the Internet Secure*. AMS Blogs, 2014. URL: https://blogs.ams.org/mathgradblog/2014/03/30/rsa/.

[Bue89] Duncan A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. New York: Springer-Verlag, 1989.

[CA21] Monica Celis Céron e Paulo Almeida. «Binary quadratic forms and the factorization method of Gauss». Mar. de 2021. URL: http://arxiv.org/abs/2103.17036.

[Coh96] Henri Cohen. *A Course in Computational Algebraic Number Theory*. English. 3.ª ed. Berlin, Heidelberg: Springer, 1996. ISBN: 3-540-55640-0.

[Dic52] Leonard Eugene Dickson. *Divisibility and Primality*. Vol. I. History of the Theory of Numbers. New York: Chelsea Publishing Company, 1952.

[Fel18] Marc Felipe i Alsina. «Binary Quadratic Forms». English. Bachelor's Thesis. Universitat Politècnica de Catalunya, 2018. URL: http://hdl.handle.net/2117/113333.

[Gau01] Carl F. Gauss. *Disqvisitiones Arithmeticae*. Leipzig: In commissis apvd Gerh. Fleischer, 1801.

[Gau86] Carl F. Gauss. *Disquisitiones Arithmeticae*. Trad. por Arthur A. Clarke; rev. William C. Waterhouse. New York, Berlin, Heidelberg, Tokyo: Springer-Verlag, 1986. ISBN: 0-387-96254-9.

[Gau95] Carl F. Gauss. *Disquisitiones Arithmeticae*. Trad. por H.B. Campos, M. Josephy e A.R. Zúñiga. Santa Fe de Bogotá, D.C.: Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 1995. URL: http://www.centroedumatematica.com/aruiz/libros/DisquisitionesArithmeticae/.

[Gee20] GeeksForGeeks. *Python Program for Extended Euclidean algorithms*. Improvements by Omnifarious. GeeksForGeeks, 2020. URL: https://www.geeksforgeeks.org/python-program-for-basic-and-extended-euclidean-algorithms-2/.

[Gra] Andrew Granville. «Gauss's Disquisitiones Arithmeticae». (First draft, comunicação pessoal).

[Gra18] Jeremy J Gray. *A History of Abstract Algebra: From Algebraic Equations to Modern Algebra*. Cham: Springer, 2018.

[GSS07] Catherine Goldstein, Norbert. Schappacher e ed. lits. Schwermer, Joachim. *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*. English. Berlin, Heidelberg: Springer-Verlag, 2007. ISBN: 978-3-540-20441-1.

[Ore48] Øystein Ore. *Number Theory and its History*. New York: McGraw-Hill, 1948.

[Res21] Wolfram Research. *Wolfram|Alpha – Computational Intelligence*. 2021. URL: `www.wolframalpha.com`.

[Ros11] Kenneth H. Rosen. *Elementary Number Theory and its Applications*. English. 6th. ed. Boston, Mass.; Munich: Pearson, 2011. ISBN: 978-0321500311.

[Ruf17] Antonio Rufián Lianza. *Gauss : A Teoria dos Números : Se os números pudessem falar*. Trad. por Fernanda Rosa. Ed. espec. 2017.

[She13] Rick L. Shepherd. «Binary Quadratic Forms and Genus Theory». English. Bachelor's Thesis. Greensboro: The University of North Carolina, 2013. URL: `https://libres.uncg.edu/ir/uncg/listing.aspx?styp=ti%5C&id=15057`.

[Sin20] Shampa Sinha. *Long Division Method to find Square root with Examples*. GeeksForGeeks, 2020. URL: `https://www.geeksforgeeks.org/long-division-method-to-find-square-root-with-examples/`.

[Smi06] Frederick J. Smith. «A Brief History of Factorization Techniques». CSE P 590TU Final Project. Washington: University of Washington, 2006. URL: `https://courses.cs.washington.edu/courses/csep590/06wi/finalprojects/smith-erick.doc`.

[Wei84] André Weil. *Number theory : an approach through history from Hammurapi to Legendre*. English. Boston: Birkhäuser, 1984. ISBN: 3-7643-3141-0.

Anexo A

Uma aplicação artesanal

De seguida, apresentamos quatro imagens que exemplificam a execução artesanal do aparelho descrito no capítulo 5. As primeiras duas imagens pretendem mostrar como o aparelho está feito, as duas últimas exemplificam duas filtragens dos candidatos a divisores dos números estudados nesta dissertação, 21037 e 997331.

Figura A.1: Varetas dos resíduos quadráticos negativos.

Figura A.2: Varetas dos resíduos quadráticos positivos

Estas varetas são feitas a partir do que comummente se denomina por 'pauzinhos de gelado'. A vareta mais à esquerda contém os números primos entre 3 e 139, a fim de efetuar a filtragem. Na primeira célula temos a letra p, para simbolizar que é a vareta dos módulos primos. As restantes varetas estão construidas como descrito no capítulo 5 com a particularidade que, cada vareta (à exceção da que corresponde a -1) tem a vareta correspondente ao inverso aditivo do cabeçalho no verso. Construimos somente as varetas com cabeçalhos livre de quadrados, como sugerido por Gauss.

Na próxima página mostramos o Crivo Gaussiano em ação para os números supramencionados. Na imagem correspondente ao processo de filtragem de 997331, usamos os resíduos quadráticos encontrados no capítulo 4 como nos foi possível.

Figura A.3: Crivo Gaussiano para 21037

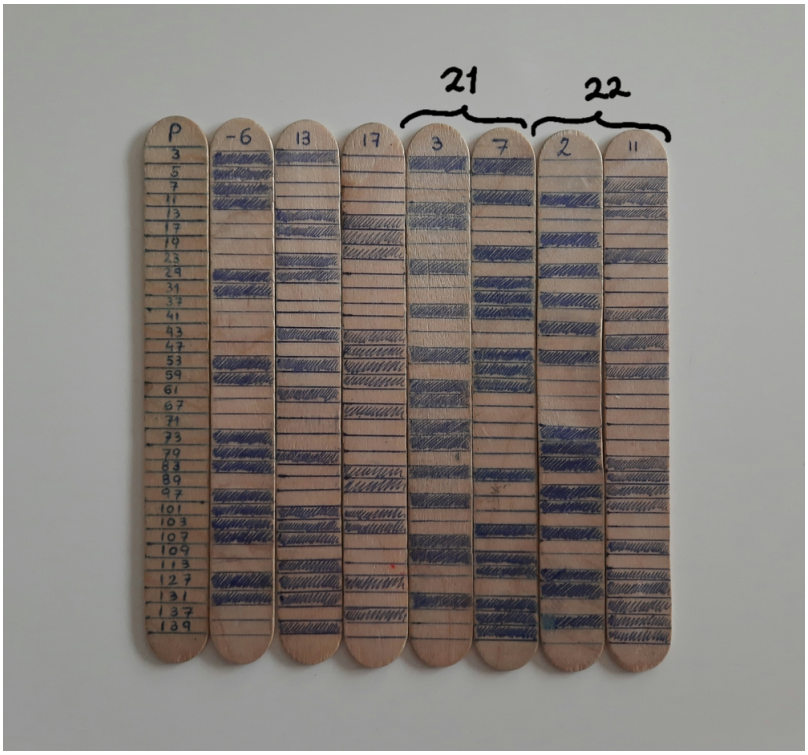

Figura A.4: Crivo Gaussiano para 997331

Anexo B

Critérios de Divisibilidade

Este anexo serve para apresentar certos critérios de divisibilidade. Mesmo sendo de conhecimento geral, poderão ser úteis na simplificação dos cálculos.

B.1 Critérios de divisibilidade e congruência

Seja N um número natural em base 10. Este pode ser escrito na forma:

$$N = \sum_{i=0}^{n} a_i \cdot 10^i.$$

Proposição B.1 (Congruência módulo 2^k)
Em módulo 2^k, N é congruente ao número formado pelos seus últimos k algarismos lidos como um número em base 10.

Demonstração. Como $10 \equiv 0 \pmod 2$, deduzimos que $10^k \equiv 0 \pmod{2^m}$, para $k \geqslant m$,

$$\begin{aligned} N = \sum_{i=0}^{n} a_i \cdot 10^i &= a_0 \cdot 10^0 + a_1 \cdot 10^1 + ... + a_k \cdot 10^k + ... + a_n \cdot 10^n \\ &\equiv a_0 \cdot 10^0 + a_1 \cdot 10^1 + ... + a_{k-1} \cdot 10^{k-1} \pmod{2^k}. \end{aligned}$$

Q.E.D.

Proposição B.2 (Congruência módulo 5^k)
Em módulo 5^k, N é congruente ao número formado pelos seus últimos k algarismos lidos como um número em base 10.

Demonstração. A prova é a mesma que a proposição anterior, substituindo 2 por 5.

Q.E.D.

Exemplo B.3
Antes de se passar a outros critérios, acompanham-se as proposições passadas com exemplos.

1. $628315 \equiv 628300 + 15 \equiv 0 + 15 \equiv 15 \pmod{5^2}$.
2. $314159 \equiv 314000 + 159 \equiv 0 + 159 \equiv 159 \pmod{2^3}$.

Proposição B.4 (Congruência módulo 3)
N é congruente à soma dos seus algarismos em módulo 3.

Demonstração. Tome-se N na forma anterior. Como $10 \equiv 1 \pmod 3$, vem:

$$N = \sum_{i=0}^{n} a_i \cdot 10^i \equiv \sum_{i=0}^{n} a_i \cdot 1^i \equiv \sum_{i=0}^{n} a_i = a_0 + a_1 + a_2 + ... + a_n \pmod 3$$

. Q.E.D.

Observação B.5 (Congruência módulo 9)
Como $10 \equiv 1 \pmod 9$, a proposição anterior também vale para módulo 9. Esta é a base para aquilo outrora conhecido como "Prova dos Nove", usada como um teste aritmético.

Proposição B.6 (Congruência módulo 11)
N é congruente à soma alternada dos seus algarismos em módulo 11.

Demonstração. O raciocínio é semelhante à proposição anterior. Como $10 \equiv -1 \pmod{11}$, vem:

$$N = \sum_{i=0}^{n} a_i \cdot 10^i \equiv \sum_{i=0}^{n} a_i \cdot (-1)^i = a_0 - a_1 + a_2 - a_3 + ... + (-1)^n \cdot a_n \pmod{11}.$$

Q.E.D.

Exemplo B.7
Antes de se passar a outros critérios, acompanham-se as proposições passadas com exemplos.

1. $628315 \equiv 5 + 1 + 3 + 8 + 2 + 6 \equiv 25 \equiv 2 + 5 \equiv 7 \pmod 3$.
2. $314159 \equiv 9 - 5 + 1 - 4 + 1 - 3 \equiv -1 \equiv 10 \pmod{11}$.

Corolário B.8 (Divisibilidade)
Sendo assim,

1. N é divisível por 2^k, se os seus últimos k algarismos são um múltiplo de 2^k.
2. N é divisível por 5^k, se os seus últimos k algarismos são um múltiplo de 5^k.
3. N é divisível por 3 se e só se a soma dos seus algarismos é um múltiplo de 3.
4. N é divisível por 11 se e só se a soma alternada dos seus algarismos é um múltiplo de 11.

Exemplo B.9
Apresenta-se umas aplicações destes critérios.

1. $628311 \equiv 6 + 2 + 8 + 3 + 1 + 1 \equiv 21 \equiv 2 + 1 \equiv 3 \equiv 0 \pmod 3$ - *É divisível por* 3.
2. $314160 \equiv 0 - 6 + 1 - 4 + 1 - 3 \equiv -11 \equiv 0 \pmod{11}$ - *É divisível por* 11.
3. $999375 \equiv 375 \equiv 0 \pmod{5^3}$ - *É divisível por* 125.
4. $3141256 \equiv 56 \equiv 0 \pmod{2^2}$ - *É divisível por* 4.

No entanto, para testar a divisibilidade por certos números não existem testes de aplicação tão simples como os vistos. Segue, de seguida, um critério iterativo com exemplos da sua aplicação.

Teorema B.10 (Critério de Divisibilidade Geral)
Seja $N = 10a + b$ para $a, b \in \mathbb{N}$ e d tal que $\text{mdc}(10, d) = 1$ e c é o inverso de 10 módulo d. Deste modo, d divide N, se e só se d divide $a + bc$.

Observação B.11
No teorema anterior, onde se usa 10, poder-se-ia considerar qualquer outro número. O número 10 é usado para aludir à base numérica com a qual é habitual escrever números inteiros.

Demonstração. Tomemos $N = 10a + b$, suponhamos que d divide N e tomemos c como definido no enunciado.

$$10a + b \equiv 0 \pmod{d} \iff c \cdot (10a) + c \cdot b \equiv a + bc \equiv 0 \pmod{d}.$$

Deste modo, d divide $a + bc$.

Q.E.D.

Divisibilidade iterativa
Baseando-se neste teorema, criamos um algoritmo para testar se um número N é divisível por um número d, automatizado em D.2.3.

Algoritmo de redução de ordem de magnítude
Seja M_0 o número a testar e seja c o inverso de 10 módulo d. 1. Calculamos $M_0 = 10a_0 + b_0$ e $N_0 = a_0 + cb_0$. 2. Caso N_0 tenha uma ordem de magnitude baixa, ou seja mais reconhecível como múltiplo de d, basta efetuar a divisão por d. Caso contrário, voltamos ao passo 1, recomeçando o processo com N_0. Iteramos o processo tantas vezes quantas forem necessárias até termos um número mais facilmente manejável.

Tabela B.1: Algoritmo de redução de ordem de magnitude para teste de divisibilidade

Exemplo B.12
Seja $N = 3164$ e queremos estudar se é divisível por 7. Podemos tomar o inverso de 10 módulo 7 como -2, pois é o representante de menor valor absoluto.

1. *Seja $M_0 = 316 \cdot 10 + 4$ e $N_0 = 316 - 2 \cdot 4 = 308$. Vem que 308 ainda não é um múltiplo aparente de 7, por isso, repetimos o processo.*
2. *Seja $N_0 = M_1 = 30 \cdot 10 + 8$ e $N_1 = 30 - 2 \cdot 8 = 14$. Podemos reconhecer 14 como múltiplo de 7, logo, o número original tem de ser múltiplo de 7.*

Observação B.13
Deixamos a cargo do leitor comprovar que usando este algoritmo como teste de divisibilidade para os primos 3 e 11, obtemos exatamente o mesmo critério.

Para ajuda do leitor, computámos valores para c para certos números primos e deixamo-los numa tabela abaixo transcrita. Estes são os valores com menor valor absoluto.

Inversos de 10	Números primos.
-2	7
4	13
-5	17
2	19
7	23
3	29
-3	31

Tabela B.2: Inversos multiplicativos de 10 em certos módulos primos

Anexo C

Técnicas de cálculo para raízes quadradas

Este anexo serve para apresentar duas formas de calcular raízes quadradas de um número N natural positivo sem o uso de calculadoras. A título de exemplo, tomemos $N = 2389$ para as seguintes técnicas. Antes de mais nada, tomemos um primeiro enquadramento usando um conhecimento prévio dos números quadrados, e podemos melhorá-lo.

$$40^2 < 2389 < 50^2. \tag{C.1}$$

C.1 Método da bisseção

Uma forma simples de estimar uma raiz quadrada é aplicar uma variante do método da bisseção.

Teorema C.1 (Bolzano)
Sejam $a, b \in \mathbb{R}$ tais que $a < b$. Se $f : [a, b] \to \mathbb{R}$ é uma função contínua t.q. $f(a) \cdot f(b) < 0$, então existe $x^* \in]a, b[$ t.q. $f(x^*) = 0$.

O método da bisseção dependerá deste teorema. A ideia é bissetar sucessivamente o intervalo[1] $[a, b]$ em meios-intervalos de modo a localizar a secção na qual se encontra o zero da função f.

Algoritmo
Seja f nas condições do Teorema de Bolzano. Para iniciar, sejam $a_0 = a$, $b_0 = b$ e $m_0 = \frac{a+b}{2}$. Podemos ter três situações: 1. $f(m_0) = 0$, então $x^* = m_0$. 2. $f(m_0) \neq 0$ e $\operatorname{sgn}(f(m_0)) = \operatorname{sgn}(f(a_0))$, então $a_1 = m_0$ e $b_0 = b_1$. 3. $f(m_0) \neq 0$ e $\operatorname{sgn}(f(m_0)) = \operatorname{sgn}(f(b_0))$, então $a_1 = a_0$ e $b_1 = m_0$. Iteramos o processo para o novo intervalo $[a_1, b_1]$ tantas vezes quantas forem necessárias.

Tabela C.1: Algoritmo da Bisseção

[1] Este e subsequentes intervalos referidos neste anexo são intervalos de números inteiros. Mais explicitamente, denotamos $[a, b]$ como o intervalo de números inteiros entre a e b, inclusive.

Para usarmos este método na estimação da raiz quadrada, temos de tomar o polinómio $f(x) = x^2 - N$, sendo N um número inteiro para o qual se quer encontrar a raiz quadrada.
No entanto, não sendo N um número quadrado, este polinómio não terá uma raiz inteira. É então necessário adaptar este método com as seguintes recomendações:

1. Uma vez que não procuramos os zeros do polinómio $x^2 - N$, mas sim aproximações inteiras aos mesmos, a nossa condição de paragem deverá ser o ponto em que o intervalo $[a, b]$ apenas contém os pontos a e b. Quando isto acontecer, teremos que $f(a) < 0$ e $f(b) > 0$ e estes serão os pontos mais próximos de $\sqrt{N}$.

   Caso encontremos zeros, significa que N é um quadrado perfeito e a fatorização torna-se bastante mais fácil

2. Como trabalhamos com intervalos discretos de números inteiros, convem proceder com cautela no que toca a considerar os pontos médios m_i. Poderá acontecer que algum ponto m_i não seja um número inteiro. Neste caso, convem avaliar a função em $\lceil m_i \rceil$ e $\lfloor m_i \rfloor$.

   Caso $\text{sgn}(f(\lceil m_i \rceil)) = \text{sgn}(f(\lfloor m_i \rfloor))$, devemos tomar o valor que nos diminuirá mais o comprimento do intervalo, de modo a chegar à solução em menos passos.

   Caso $\text{sgn}(f(\lceil m_i \rceil)) \neq \text{sgn}(f(\lfloor m_i \rfloor))$, podemos parar a nossa busca aqui pois acabámos de demonstrar que o zero da função $x^2 - N$ está no intervalo $[\lfloor m_i \rfloor, \lceil m_i \rceil]$ o qual é um intervalo de números inteiros com 2 elementos. É impossível bissetar mais este intervalo de modo a que contenha somente números inteiros.

Exemplo C.2
Queremos estimar $\sqrt{2389}$. *Usando o enquadramento (C.1), consideremos o intervalo* $[40, 50]$. *Começamos com*

$a_0 = 40$	$b_0 = 50$	$m_0 = \frac{40+50}{2} = 45$
$f(a) = 40^2 - 2389 = -789 < 0$	$f(b) = 50^2 - 2389 = 111 > 0$	$f(m_0) = 45^2 - 2389 = -364 < 0$

Como $\text{sgn}(f(m_0)) = \text{sgn}(f(a))$, *vem que* $a_1 = m_0$ *e* $b_1 = b_0$. *Retomamos com o intervalo* $[45, 50]$. *Um cálculo simples mostra que* $m_1 = \frac{45+50}{2} = 47,5$. *Aqui convem proceder com cautela pois* $m_1 \notin \mathbb{Z}$. *Uma vez que* $\text{sgn}(f(\lfloor m_1 \rfloor)) = \text{sgn}(f(\lceil m_1 \rceil))$, *escolhemos* $\lceil m_1 \rceil$ *como novo ponto médio pois minimiza o comprimento do intervalo seguinte.*

$a_1 = 45$	$b_1 = 50$	$m_1 = \lceil \frac{45+50}{2} \rceil = 48$
$f(a) = 45^2 - 2389 = -364 < 0$	$f(b) = 50^2 - 2389 = 111 > 0$	$f(m_1) = 48^2 - 2389 = -85 < 0$

Como $\text{sgn}(f(m_1)) = \text{sgn}(f(a_1))$, *atualizamos os valores* $a_2 = m_1$ *e* $b_2 = b_1$. *Retomamos com o intervalo* $[48, 50]$. *Calculamos o ponto médio novamente e temos* $m_2 = \frac{48+50}{2}$.

$a_2 = 48$	$b_2 = 50$	$m_2 = 49$
$f(a) = 48^2 - 2389 = -85 < 0$	$f(b) = 50^2 - 2389 = 111 > 0$	$f(m_2) = 49^2 - 2389 = 12 > 0$

Neste caso, $\operatorname{sgn}(f(m_2)) = \operatorname{sgn}(f(b_2))$. *Logo, atualizamos os valores para* $b_3 = m_2$ *e* $a_3 = a_2$. *Já não é necessário calcular o ponto médio entre estes números, pois já obtemos um intervalo de números inteiros contendo apenas 2 elementos inteiros pelo que será impossível descobrir mais soluções inteiras fazendo subdivisões.*

$$2389 = 48^2 + 85 = 49^2 - 12.$$

C.2 Divisão

A ideia deste método aproximarmo-nos progressivamente de uma boa estimativa para $\sqrt{N}$. Tomamos $a > 0$ uma primeira aproximação para $\sqrt{N}$ e $r > 0$. No turno seguinte, queremos que $a + r$ seja uma melhor aproximação. A observação em que se fundamenta este método é

Observação C.3 (Minorar a raiz)
Através de uma conta simples, temos a base deste método

$$\begin{aligned} a + r \leqslant \sqrt{N} &\implies (a+r)^2 \leqslant N && \text{(C.2)} \\ &\iff a^2 + 2ar + r^2 \leqslant N && \text{(C.3)} \\ &\iff 2ar + r^2 \leqslant N - a^2 && \text{(C.4)} \\ &\iff (2a + r)r \leqslant N - a^2. && \text{(C.5)} \end{aligned}$$

A cada iteração tomamos o maior r inteiro que verifica esta condição. Este método permite-nos construir a raiz quadrada dígito-a-dígito começando pelo elemento de maior magnitude, não sendo totalmente necessário usar um enquadramento prévio como o enquadramento (C.1).

Exemplo C.4
Querendo encontrar $\sqrt{2389}$, *conseguimos ter uma primeira aproximação usando o enquadramento (C.1). Supondo que temos* 4 *como primeiro dígito, vem*

$$\begin{aligned} 40 + r < \sqrt{2389} &\implies (40+r)^2 \leqslant 2389 \\ &\iff 40^2 + 80r + r^2 \leqslant 2389 \\ &\iff 80r + r^2 \leqslant 789 \iff (80+r)r \leqslant 789. \end{aligned}$$

Podemos experimentar valores de modo a chegar a:

$$\begin{aligned} r = 8 &\implies (80+8)\cdot 8 \leqslant 789 \\ r = 9 &\implies (80+9)\cdot 9 > 789. \end{aligned}$$

Tomamos 48 *como a próxima aproximação para* $\sqrt{2389}$. *Tal como antes, concluimos:*

$$2389 = 48^2 + 85 = 49^2 - 12.$$

Podemos notar que, pela condição de minoração na inequação (C.5), as estimativas para a raiz usando esta técnica serão sempre para $\lfloor \sqrt{N} \rfloor$. Uma implementação deste método era ministrada no ensino obrigatório há algumas decadas. Mostramo-la abaixo usada para o mesmo número.

Raiz quadrada através de divisões sucessivas

A primeira parte é separar o número em grupos de 2 algarismos a começar pela direita. Para clarificar, um número como 2389 é tratado como 23 | 89. Caso o número de algarismos de um número seja ímpar, o grupo mais à esquerda fica com apenas um algarismo. Portanto, um número como 14142 é tratado como 1 | 41 | 42. De modo a conseguir explicar este algoritmo de forma concreta, partimos de um exemplo elucidativo, neste caso queremos calcular $\sqrt{2389}$. Alinhamos o número em questão numa tabela do seguinte modo:

$$\begin{array}{|l} \hline 23 \mid 89 \\ \\ \end{array}$$

Em seguida, consideramos o grupo mais à esquerda como o número 23 e subtraimos-lhe o maior número quadrado de modo a ter um resultado positivo. Como $4^2 < 23 < 5^2$, então $23-4^2 = 7 > 0$. Escrevemos o número 4, por cima da barra horizontal e à esquerda da barra vertical. O resultado da subtração é posto sob o grupo ao qual se subtraiu.

$$\begin{array}{rl} & 4 \\ \hline 4 & 23 \mid 89 \\ & 7 \\ \\ \end{array}$$

Descemos o seguinte grupo e lemos a segunda linha como um número - neste caso, o 789. Neste momento, na observação C.3, encontramo-nos no passo (C.4).

$$\begin{array}{rl} & 4 \\ \hline 4 & 23 \mid 89 \\ & 7 \quad 89 \\ \\ \end{array}$$

Observação C.5
É digno de nota que este 4 não tem o peso de 4 mas sim de 40 uma vez que fazemos as contas da esquerda para a direita e há 2 grupos ($40 = 4 \cdot 10^{\mathbf{2}-1}$). (Caso houvesse 3 grupos, este número teria o peso de 400, pois $400 = 4 \cdot 10^{\mathbf{3}-1}$).

Deste modo, vemos que obtemos a mesma minoração presente no enquadramento (C.1). É uma força especial deste método não precisar de se ter um enquadramento prévio.

Para encontrar o próximo dígito, duplicamos a aproximação 40 situada sobre a barra horizontal e obtemos 80. Como tal, à esquerda da barra vertical, escrevemos 8 com um espaço em branco. Como expresso na observação C.3, estamos no passo (C.5). O objetivo agora será encontrar um algarismo r tal que $(80 + r) \cdot r$ esteja o mais perto de 789 possível, sem o superar.

$$\begin{array}{rl} & 4 \\ \hline 4 & 23 \mid 89 \\ 8\_ & 7 \quad 89 \\ \\ \end{array}$$

Pelas contas anteriores, sabemos que este dígito é 8. Completamos com 8 à esquerda da linha vertical e por cima da linha horizontal a seguir ao 4. Subtraimos $88 \cdot 8 = 704$ a 789 e escrevemos o resultado sob o número 789. Neste caso, é igual a 85.

$$\begin{array}{rr|l} & 4\ \ 8 & \\ \hline 4 & 23 & 89 \\ 88 & 7\ \ & 89 \\ & & 85 \end{array}$$

Deste modo, analisando esta tabela, obtemos logo os dados necessários a poder minorar $\sqrt{2389}$. Assim, podemos escrever

$$2389 = 48^2 + 85 = 49^2 - 12$$

Para continuar o processo e obter uma aproximação mais exata para $\sqrt{2389}$ e obter a primeira casa decimal teriamos de acrescentar 2 zeros à direita e tratá-los como parte integrante do número. A partir daqui, podemos proceder como já vimos e assim por diante.

Este algoritmo está explicado e tratado em [Sin20].

Anexo D

Códigos

Neste anexo exibimos uma forma de executar o código criado para esta dissertação. Este procedimento foi criado para o sistema operativo *Windows*, mas também serve para os sistemas *Linux* e *iOS*, com as devidas adaptações. O esquema será o mesmo para os três sistemas operativos indicados. Transcrevemos os comandos necessários a adaptar para *Linux* e *iOS* na secção D.4.

D.1 Burocracias de instalação

Este é o procedimento geral feito para Windows que poderá ser adaptado para iOS e Linux (ver secção D.4). Antes de tudo, é necessário que o leitor instale uma versão da linguagem de programação Python[1], numa versão tão ou mais recente que a versão 3.6. Em seguida, o leitor tem duas opções para obter o código desta dissertação no seu computador.

1. Descarregar o código já publicado no repositório *GitHub*: `https://github.com/ghaleon7/FQB_Gauss`, em formato 'zip'.
2. Criar os ficheiros de raiz na sua máquina e escrever o código-fonte que está na secção D.2, em cada ficheiro.

Seja qual for a forma que o leitor escolher, precisamos de entender a organização da biblioteca criada. O código programado está contido numa pasta com o nome `Gauss_QF`, a qual[2] contém os seguintes quatro ficheiros.

`Gauss_QF`

- `__init__.py`
- `Gauss_QF.py`
- `_GaussUtils.py`
- `primos_div.py`

Devido a usarmos *imports* relativos, a organização dos ficheiros tem mesmo de ser esta. Dado que uma pasta está quase sempre dentro de outra pasta, suponhamos que a pasta `Gauss_QF` está dentro de uma pasta cujo caminho é representado por `%pastaAnterior%`.

[1] Pode ser até em distribuições como o Anaconda.

[2] Mesmo que o utilizador escolha a opção 2 da instalação, sugerimos que a pasta criada mantenha este nome.

Apresentamos 2 exemplos de caminhos que podem ser representados por `%pastaAnterior%`:

- Caso o utilizador tenha a pasta `Gauss_QF` no Desktop, então `%pastaAnterior%` poderá ser o caminho `C:\Users\utilizador\Desktop`, na qual `utilizador` é o nome do usuário que o leitor terá na sua máquina.
- Caso o utilizador tenha decidido descarregar o código diretamente do *GitHub*, então a pasta que contém a pasta `Gauss_QF` terá o nome `FQB_Gauss-main` e o caminho completo será algo como `C:\Users\utilizador\Downloads\FQB_Gauss-main\FQB_Gauss-main`, caso o leitor descarregue a pasta para os `Downloads`

Caso o leitor tenha escolhido criar os ficheiros de raiz, será necessário consultar a secção D.2 antes de continuarmos. Caso contrário, continue a ler.

Uma vez descarregada a pasta 'zipada' do *GitHub*, precisamos de extrair os seus ficheiros. Agora, queremos abrir a linha de comandos. Vamos abrir um terminal na pasta `%pastaAnterior%` . À data de escrita desta dissertação, no *Windows* 10, isto pode ser feito de uma de duas formas:

- Invocar a linha de comandos e escrever o comando `cd %pastaAnterior%`.
- Entrar nas pastas extraídas e navegar até à pasta imediatamente anterior à pasta `Gauss_QF`, ou seja, a pasta com o caminho `%pastaAnterior%`. Nesta pasta, na barra superior que indica o caminho para a pasta, escrever `cmd` e premir *Enter*.

Depois de efetuar uma das duas ações anteriores, teremos a linha de comandos[3] com a referência da pasta `%pastaAnterior%` . Agora falta criar o ambiente virtual no qual vamos trabalhar. Nos comandos seguintes, caso o utilizador se depare com uma mensagem de erro, experimente substituir `py` por `python`. Para criar o ambiente virtual chamado 'gauss', digitamos:

```
py -m venv gauss
```

O nome `gauss` é opcional. Se o utilizador desejar utilizar um nome diferente, no passo seguinte tem de ser usado o mesmo nome. De seguida, após criar o ambiente, é necessário ativá-lo. Para tal, digitamos:

```
.\gauss\Scripts\activate
```

Se o utilizador analisar o código-fonte transcrito na secção D.2, podemos reparar na instrução

```
import numpy as np.
```

Assim, teremos de instalar o `numpy`. Para tal, digitamos na linha de comandos:

```
pip install numpy
```

[3]Caso o utilizador escolha instalar o Python usando a distribuição Anaconda ou semelhante, será necessário abrir a linha de comandos desta distribuição (*Anaconda Prompt* no *Windows*) e escrever o comando `cd` %`pastaAnterior`%. Neste caso, em vez de escrevermos o comando `py`, escreveremos `python`.

Caso o utilizador não possa instalar a versão mais recente do numpy, sugerimos somente uma versão tão ou mais recente que a versão 1.10. Por fim, basta apenas ativar o Python através do comando

```
py
```

Como foi dito, se o comando `py` não funcionar, será necessário tentar `python`. Agora estamos a postos para usar o código aqui exposto! Para que o utilizador conheça cada ficheiro e as funções que estão programadas, aconselhamos uma inspeção da secção D.2. No mínimo, saber os nomes das funções que estão programadas. Cada função está documentada, e a sua documentação inclui exemplo de uso. Finalmente, apresentamos indicações e sugestões de uso, adiante, na secção D.3.

D.2 Código-fonte e criação de raiz

O início desta secção é dirigido a quem decidiu criar os ficheiros de raiz. Nesta forma de instalação, vamos criar os ficheiros de código de raiz, para o caso de o acesso ao repositório *GitHub* ser limitado.
Começamos por criar uma pasta à qual vamos dar o nome `Gauss_QF`. Dentro da pasta criamos quatro ficheiros. Podemos criar estes ficheiros usando uma aplicação semelhante ao *Bloco de Notas* e mudando os seus nomes para

```
__init__.py, Gauss_QF.py, _GaussUtils.py, primos_div.py .
```

Note-se que a extensão original também terá de ser mudada. De seguida, editamos cada ficheiro escrevendo o código-fonte transcrito correspondente que se segue.

Cautela! Caso o leitor opte por copiar o código adiante transcrito, será necessário ter presente que o código poderá não ter as indentações mostradas, pelo que o utilizador terá de fazê-las manualmente com a tecla de Parágrafo (TAB) e Mudança de Linha (ENTER). Também, é preciso considerar que há funções neste documento que mudam de página e o número de página pode provocar erros.

D.2.1 Indicação de *package*

De forma a que esta pasta seja lida como uma *package*, será útil que contenha um ficheiro `__init__.py`.

Conteúdo do ficheiro `__init__.py`:

```
from .Gauss_QF import Gauss_QF
from .primos_div import prod, prime_lst, divm
```

D.2.2 Funções auxiliares

As funções do ficheiro `_GaussUtils.py` são funções auxiliares para serem usadas por ambos os *scripts* principais `primos_div.py` e `Gauss_QF.py`.

Conteúdo do ficheiro `_GaussUtils.py`:

```
import numpy as np
def gcdxy(a, b):
    """
    Esta função calcula o máximo divisor comum entre a e b
    de forma a resolver a equação ax + by = mdc(a,b).
    Baseado em: https://www.geeksforgeeks.org/python-program-
    for-basic-and-extended-euclidean-algorithms-2/
    Argumentos:
        - a,b - int
    Devolve:
        - gcd, x, y - int
    Exemplo:
        gcdxy(15,8)
            >> (1, -1, 2)
    """
    if a == 0 :
        return b,0,1
    gcd,x_i,y_i = gcdxy(b%a, a)
    x,y = y_i - (b//a) * x_i, x_i
    return gcd,x,y

def int_converter(*args):
    """
    Esta função serve para converter floats que também são inteiros
    em inteiros.
    Argumentos:
        a,b,c - números inteiros
    Devolve:
        (a,b,c) - vetor de inteiros
    Exemplo:
        int(1.0, 2.0, 3.0)
            >> (1,2,3)
    """
    args = list(args)
    if all([isinstance(x,(int, np.int32, np.int64)) for x in args]):
        return tuple(args)
    elif any([isinstance(x,(float, np.float32, np.float64)) for x in args]):
        i = 0
        while i < len(args):
            if isinstance(args[i], (int, np.int32, np.int64)):
                args[i] = args[i]
            elif args[i].is_integer():
```

```
                args[i] = int(args[i])
            i+=1
        return tuple(args)

def verify(*args):
    """
    Esta função serve para verificar se as instâncias estão bem inicializadas.
    Se fizermos como F = QF(pi,2,3), ou F = QF(1.0, 2.0, 3.0) lança TypeError.
    Argumentos:
        a,b,c - ints
    Devolve:
        bool
    Exemplos:
        verify(np.pi,2,3)
            >> TypeError: Foi introduzido um número não-inteiro
        verify(1,2,3)
            >> True
    """
    #Isto acautela que todas as instâncias são inteiros
    args = list(args)
    if not all([isinstance(x,(int, np.int32, np.int64)) for x in args]):
        raise TypeError("Foi introduzido um número não-inteiro")
    else:
        return True

def b_abs_min(b,a):
    """
    Método auxiliar que calcula o congruente absoluto mínimo
    de um número -b módulo a. Usa-se no método reducing para formas de
    determinante negativo
    """
    res = -b % a
    res_1 = res - a
    x = min(abs(res), abs(res_1))
    if x == abs(res):
        return res
    else:
        return res_1

def b_sqrt(b, a, lim_inf, lim_sup):
    """
    Método auxiliar que calcula o representante de um número b módulo a
    Usa-se no método reducing para formas de determinante positivo
    """
```

```
    res = (-b)%a
    while res < lim_inf:
        res = res + abs(a)
    while lim_sup < res:
        res = res - abs(a)
    return res
```

D.2.3 Funções diversas

O ficheiro `primos_div.py` contém funções diversas que cumpriram fins não diretamente relacionados com os trabalhos de Gauss. Sendo assim, julgámos ser mais simples que tivessem num ficheiro à parte. Neste ficheiro figuram as funções `prod` e `prime_lst` que foram usadas para calcular a percentagem de números não divisíveis por um primo abaixo de 100, 139 e de 1000 na subsecção 5.4. Também temos a função `divm` que executa o teste de divisibilidade delineado no anexo B.

Conteúdo do ficheiro `primos_div.py`:

```
import numpy as np
from numpy import sqrt as sq
from ._GaussUtils import gcdxy

def prod(lst):
    """
    Esta função calcula o produto de todos os elementos de uma lista.
    Argumentos:
        lst - list
    Devolve:
        p - int
    Exemplo:
        prod([1,2,3]):
            >>> 6
    """
    if not isinstance(lst, list):
        raise TypeError(f"O utilizador introduziu um argumento {type(lst)}," +\
                        " precisamos que seja uma lista.")
    p = 1
    for i in lst:
        p *=i
    return p
```

```
def prime_lst(upper):
    """
    Esta função permite obter uma lista dos números primos de 2
    até um limite superior dado.
    Argumentos:
        - upper: limite superior; int
    Devolve:
        - lst: lista de primos até ao limite superior
    Exemplos:
        - prime_lst(10):
            >> [2,3,5,7]
    """
    if not isinstance(upper, (int, np.int32, np.int64)):
        raise TypeError("Precisamos de um limite superior inteiro.")
    if upper > 100000:
        raise ValueError("O limite superior deve ser inferior a 100000")
    lst = []
    for nr in range(2, upper + 1):
       for i in range(2, int(sq(nr))+1):
           if (nr % i) == 0:
               break
           else:
               lst.append(nr)
    return lst

def divm(n,d):
    """
    Executa o teste de divisibilidade. n é o inteiro a testar,
    d é o possível divisor. Supomos que n está escrito em base 10.
    Argumentos:
        - n,d - int
    Devolve:
        - stry - string
    Exemplo:
        divm(15,7)
            >> "O número 15 não é divisivel por 7."
    """
    if gcdxy(10,d)[0] != 1:
        raise TypeError("O divisor tem de ser coprimo com 10.")
    else:
        a = n//10
        b = n%10
        inv = gcdxy(10,d)[1]
```

```
        N = abs(a + inv*b)
        while N > 10:
            a = N//10
            b = N%10
            N = abs(a + inv*b)
        div = N%d
        if bool(div):
            stry = "O número {} não é divisivel por {}.".format(n,d)
            return stry
        else:
            stry = "{} = {}*{}".format(n,n//d,d)
            return stry
```

D.2.4 Classe de formas quadráticas binárias

Para esta dissertação, programámos uma classe em Python de forma a poder trabalhar com as formas quadráticas binárias como objetos e com os algoritmos que lhes associámos ao longo desta dissertação.

Conteúdo do ficheiro `Gauss_QF.py`:

```
"""
Esta classe procura definir e tratar as formas quadráticas binárias como as
estudou Carl Friedrich Gauss.
Estudamos os polinómios de 2 variáveis: ax^2 + 2bxy + cy^2.
Nesta classe temos feito:
    - Operações fundamentais entre formas quadráticas binárias
    - Representação como tuplo e como matriz
    - Determinante e discriminante
    - Mudança de coordenadas por via de transformações lineares
    - Algoritmos de redução de formas quadráticas
    - Tipo de forma quadrática (definida positiva, definida negativa, indefinida)
    - Composição de formas quadráticas com determinante negativo
"""

import numpy as np
from numpy import sqrt as sq
from ._GaussUtils import gcdxy, int_converter, verify, b_abs_min, b_sqrt

############## DEFINIÇÃO DA CLASSE ################
class Gauss_QF:
    def __init__(self,a,b,c):
        """
        Esta classe trata de formas quadráticas binárias.
```

```
        Argumentos:
            a,b,c - ints
        Exemplo:
            f = Gauss_QF(3,1,332444)
        """
        args = [a,b,c]
        if not all([isinstance(x,(int, float, np.float16, np.float32,
                                  np.float64,np.int16, np.int32, np.int64)
                                ) for x in args]):
            raise TypeError("Foi um símbolo não-numérico")
        x = int_converter(a,b,c)
        if verify(*x):
            self.a,self.b,self.c = x
        else:
            raise TypeError("Necessitamos de coeficientes inteiros!")

    @classmethod
    def from_matrix(cls, matrix):
        """
        Este método recebe uma matriz simétrica e identifica-a com uma
        forma quadrática binária.
        Argumentos:
            matrix - A matriz da forma quadrática; list, np.array
        Devolve:
            f_matrix - A forma quadrática associada; Gauss_QF
        Exemplo:
            f = np.array([[1, 1],
                          [1, 3]])
            g = Gauss_QF.from_matrix(f)
            print(g)
                >> A forma quadrática é (1,1,3) e
                    é interpretada como: 1x^2+2xy+3y^2
        """
        if not isinstance(matrix, np.ndarray):
            raise TypeError("O nosso objecto deve ser uma matriz")
        elif matrix.shape != (2,2):
            raise TypeError("A matriz deve ser do tipo 2x2")
        elif not np.allclose(matrix,matrix.T):
            raise ValueError("Queremos uma matriz simétrica")
        f_matrix = cls(int(matrix[0][0]),
                       int(matrix[0][1]),
                       int(matrix[1][1]))
        return f_matrix
```

```
    @classmethod
    def from_tuple(cls, tupl):
        """
        Este método recebe um tuplo ou lista com 3 elementos e identifica-o
        com uma forma quadrática binária.
        Argumentos:
            tupl - O terno com os coeficientes da forma; list, tuple
        Devolve:
            cl_tuple - Uma forma quadrática Gauss_QF(a,b,c)
        Exemplo:
            t = (1,2,3)
            g = Gauss_QF.from_tuple(t)
            print(g)
            >> A forma quadrática é (1,2,3) e é interpretada
                como: 1x^2+4xy+3y^2
        """
        if not isinstance(tupl, (tuple,list)):
            raise TypeError("O nosso objecto deve ser um tuplo ou lista")
        if len(tupl) !=3:
            raise TypeError("O nosso objeto deve ter 3 elementos")
        cl_tuple = cls(tupl[0], tupl[1], tupl[2])
        return cl_tuple

    @property
    def determinant(self):
        """
        Este método calcula o determinante de uma forma quadrática.
        Devolve:
            - determinant - o determinante da forma quadrática; int
        Exemplo:
            f = Gauss_QF(1,2,3)
            f.determinant
                >> 1
        """
        determinant = (self.b)**2 - (self.a)*(self.c)
        return determinant
```

```
    @property
    def discriminant(self):
        """
        Este método calcula o discriminante de uma forma quadrática.
        Devolve:
            - discriminant - o discriminante da forma quadrática; int
        Exemplo:
            f = Gauss_QF(1,2,3)
            f.discriminant
                >> 4
        """
        discriminant = 4*(self.b)**2 - 4*(self.a)*(self.c)
        return discriminant

    @property
    def rep_tuple(self):
        """
        Devolve a representação de uma forma quadrática binária como um tuplo.
        Devolve:
            f - A representação da forma quadrática como um terno; tuple
        Exemplo:
            f = Gauss_QF(1,2,3)
            f.rep_tuple
                >> (1,2,3)
        """
        f = (self.a, self.b, self.c)
        return f

    @property
    def rep_matrix(self):
        """
        Este método calcula a representação matricial de uma forma
        quadrática binária.
        Devolve:
            F - A representação matricial da forma quadrática; np.array
        Exemplo:
            f = Gauss_QF(1,2,3)
            f.rep_matrix
                >> array([[1, 2],
                          [2, 3]])
        """
        F = np.array([[self.a, self.b], [self.b, self.c]])
        return F
```

```
    @property
    def is_reduced(self):
        """
        Testa se uma forma quadrática é reduzida.
        Devolve:
            bool - Caso seja reduzida, deve devolver True.
                    False, caso contrário
        Exemplo:
            f = Gauss_QF(1,3,3)
            f.is_reduced
                >> False
        """
        if self.determinant < 0:
            cond_a = abs(2*self.b) <= abs(self.a) <= abs(self.c)
            cond_b = abs(self.a) <= sq(4*abs(self.determinant)/3)
            if cond_a and cond_b:
                return True
            else:
                return False
        else:
            if sq(self.determinant).is_integer():
                raise ValueError("O determinante não pode ser quadrado.")
            d = self.determinant
            cond_a = sq(d)-(self.b) <= abs(self.a) <=sq(d)+(self.b)
            cond_b = 0 < self.b <= sq(d)
            if cond_a and cond_b:
                return True
            else:
                return False

    def values(self, x, y):
        """
        Avalia o valor da forma quadrática f em (x,y), i.e., calcula f(x,y)
        Argumentos:
            x,y - Os objetos dos quais queremos calcular a imagem; int
        Devolve:
            res - A imagem da forma quadrática por x e y; int
        Exemplo:
            f = Gauss_QF(1,2,1)
            f.values(1,1)
                >> 4
        """
        coef_vect = [x,y]
```

```
        if not all([isinstance(i,(int, np.int32, np.int64))
                    for i in coef_vect]):
            raise TypeError("Procuramos inteiros.")
        res = (self.a)*x**2 + 2*(self.b)*x*y + (self.c)*y**2
        return res

    def reducing(self):
        """
        Método auxiliar que executa o algoritmo de redução de Gauss
        mostrando alguns cálculos intermédios. No processo calcula o
        processo de redução de uma forma quadrática binária.
        Argumentos:
            - self: a forma quadrática binária
        Devolve:
           - Dicionário com 3 entradas: Forma, Progressão, Comprimento
        Exemplo:
            - f = Gauss_QF(5,6,10)
            - print(f.reducing())
                >> {'Forma':(6,2,9),
                    'Progressão':{'Forma_0':(9,7,11),
                                  'Forma_1':(11,4,6),
                                  'Forma_2':(6,2,9)},
                    'Comprimento': 3}
        """
        red = [self.a, self.b, self.c]
        res_dict = {'Forma': '0', 'Progressão':'0', 'Comprimento':'0'}
        progression = [tuple(red)]
        if self.is_reduced:
            res_dict['Forma'] = tuple(red)
            res_dict['Progressão'] = progression
            res_dict['Comprimento'] = 1
            return res_dict
        else:
            i = 1
            if self.determinant < 0:
               while not Gauss_QF(*red).is_reduced:
                    red[0] = red[2]
                    red[1] = b_abs_min(red[1], red[0])
                    red[2] = int((red[1]**2 - self.determinant)/red[0])
                    progression.append(tuple(red))
                    i+=1
               res_dict['Forma'] = tuple(red)
               res_dict['Progressão'] = progression
```

```
                res_dict['Comprimento'] = i
                return res_dict
            if self.determinant >= 0:
                if sq(self.determinant).is_integer():
                    raise TypeError("O determinante não pode ser quadrado.")
                d = self.determinant
                while not Gauss_QF(*red).is_reduced:
                      red[0] = red[2]
                      red[1] = b_sqrt(red[1], red[0], sq(d)- red[0], sq(d))
                      red[2] = int((red[1]**2 - d)/red[0])
                      progression.append(tuple(red))
                      i+=1
                res_dict['Forma'] = tuple(red)
                res_dict['Progressão'] = progression
                res_dict['Comprimento'] = i
                return res_dict

    @property
    def reduced(self):
        """
        Usa a função reducing para devolver uma forma quadrática
        reduzida propriamente equivalente a f.
        Devolve:
            - f: A forma quadrática binária reduzida; Gauss_QF
        Exemplos:
            f = Gauss_QF(5,6,10)
            print(f.reduced())
                >> 'A forma quadrática é (6,2,9) e é interpretada
                    como: 6x^2+4xy+9y^2'
        """
        prog = self.reducing()
        f = Gauss_QF(*prog['Forma'])
        return f
```

```
    def period(self):
        """
        Calcula o período de uma forma quadrática binária de
        determinante positivo. Devolve uma lista com duas listas:
            - O processo de redução a uma forma quadrática reduzida
            - O período da forma quadrática reduzida equivalente à original
        Devolve:
            progression - list
        Exemplo:
            Gauss_QF(2,4,7).period()
                >> [[(2, 4, 7), (7, -4, 2), (2, 0, -1), (-1, 1, 1)],
                [(1, 1, -1), (-1, 1, 1)]]
        """
        if self.determinant < 0:
            raise TypeError(
            "O conceito de período não existe para determinante negativo.")
        elif sq(self.determinant).is_integer():
            raise ValueError("O determinante não pode ser quadrado.")
        else:
            cap = self.reducing()['Progressão']
            red, ori = list(cap[-1]), list(cap[-1])
            d = self.determinant
            progression = []
            while not tuple(red) in progression:
                ori[0] = ori[2]
                ori[1] = b_sqrt(ori[1], ori[0], sq(d)- ori[0], sq(d))
                ori[2] = int((ori[1]**2 - d)/ori[0])
                progression.append(tuple(ori))
            progression.pop()
            progression.insert(0, tuple(red))
            return [cap, progression]

    def transform_linear(self, a_11, a_12, a_21, a_22):
        """
        Este método calcula a mudança de coordenadas
        de uma forma quadrática binária.
        Argumentos:
            a_11,a_12,a_21,a_22 - Entradas da matriz de
                                  mudança de coordenadas; int
        Exemplos:
            g = Gauss_QF(1,0,1)
            h_0 = g.transform_linear(1,1,1,1)
            print(h_0)
```

```
            >> A forma inserida é (6,12,6) e é interpretada como:
                6x^2 + 24xy + 6y^2
        """
        if verify(*int_converter(a_11, a_12, a_21, a_22)):
            matM = np.array([[a_11,a_12],[a_21,a_22]])
            transformed = ((matM.T).dot(self.rep_matrix)).dot(matM)
        trans_a = int(transformed[0][0])
        trans_b = int(transformed[0][1])
        trans_c = int(transformed[1][1])
        transformed_tuple = self.__class__(trans_a,trans_b,trans_c)
        return transformed_tuple

    @property
    def typus(self):
        """
        Este método avalia se uma forma quadrática binária é definida,
        semidefinida ou indefinida.
        Exemplo:
            f = Gauss_QF(1,2,3)
            f.typus
                >> 'A forma inserida é definida positiva'
        """
        if self.discriminant > 0:
            return 'A forma inserida é indefinida'
        elif self.discriminant == 0:
            return 'A forma inserida é semidefinida'
        else:
            if self.a > 0:
                return 'A forma inserida é definida positiva'
            else:
                return 'A forma inserida é definida negativa'
```

```
#################### OPERAÇÕES COM FORMAS #############

    def is_equal(self, other):
        """
        Criamos um objecto product iterável, o qual consiste em todos
        os pares de índices possíveis. Em seguida, verificamos se a
        representação matricial de ambas as formas quadráticas corresponde.
        Exemplo:
           f,g = Gauss_QF(1,2,3), Gauss_QF(1,2,3)
           f == g
               >> True
        """
        if not isinstance(other, self.__class__):
            raise TypeError("A forma inserida não é instância da classe")
        product_indices = ((x,y) for x in [0,1] for y in [0,1])
        truth_value = all([self.rep_matrix[i][j] == other.rep_matrix[i][j]
                for (i,j) in product_indices])
        return truth_value

    def __eq__(self, other):
        """
        Definimos o que significa duas instâncias da classe serem iguais.
        """
        return self.is_equal(other)

    def add_forms(self, other):
        """
        Este método soma 2 instâncias da classe e devolve a
        sua representação matricial.
        Exemplos:
            f, h = Gauss_QF(1,2,3), Gauss_QF(3,5,6)
            f + h
                >> array([[4, 7],
                          [7, 9]])
        """
        if not isinstance(other, self.__class__):
            raise TypeError("A forma inserida não é instância da classe")
        product_indices = ((x,y) for x in [0,1] for y in [0,1])
        add = np.array([self.rep_matrix[i][j] + other.rep_matrix[i][j]
                        for (i,j) in product_indices])
        add2 = np.array([[add[0], add[1]], [add[2], add[3]]])
        return add2
```

```
    def __add__(self,other):
        """
        Definimos o que significa somar duas instâncias da classe.
        """
        return self.add_forms(other)

    def subtract_forms(self, other):
        """
        Este método subtrai 2 instâncias da classe.
        Devolve a sua representação matricial.
        Exemplos:
            f, h = Gauss_QF(1,2,3), Gauss_QF(3,5,7)
            f - h
                >> array([[-2, -3],
                          [-3, -4]])
        """
        if not isinstance(other, self.__class__):
            raise TypeError("A forma inserida não é instância da classe")
        product_indices = ((x,y) for x in [0,1] for y in [0,1])
        sub = np.array([self.rep_matrix[i][j] - other.rep_matrix[i][j]
                        for (i,j) in product_indices])
        sub2 = np.array([[sub[0], sub[1]], [sub[2], sub[3]]])
        return sub2

    def __sub__(self,other):
        """
        Definimos o que significa subtrair duas instâncias da classe.
        """
        return self.subtract_forms(other)

    def __str__(self):
        """
        Este método permite obter uma representação de uma forma
        quadrática em string. Devolve uma mensagem com a representação
        do tuplo e o polinómio em duas variáveis a que está associado.
        """
        x = (self.a,self.b,self.c)
        a,b,c = self.a,2*self.b,self.c
        if self.b >= 0:
            b = "+{}".format(b)
        if self.c >= 0:
            c = "+{}".format(c)
        y = (a,b,c)
        s1 = "A forma quadrática é ({},{},{}) ". format(*x)
```

```
        s2 = "e é interpretada como: {}x^2{}xy{}y^2".format(*y)
        return s1 + s2

    def compose(self, other):
        """
        Implementa o algoritmo de Shanks para a composição de formas
        com determinante negativo. A forma resultante pode não ser
        reduzida, pelo que será necessário usar a função reduced
        para obter uma forma reduzida propriamente equivalente.
        Este algoritmo é uma implementação do algoritmo em
        A Course in Computational Algebraic Number Theory,
        de Henri Cohen. 3.ªed.Berlin, Heidelberg: Springer, 1996, p. 247
        Argumentos:
            - self, other: duas formas quadráticas a compor;
                           Gauss_QF
        Devolve:
            - composed: a forma quadrática resultante;
                           Gauss_QF
        Exemplo:
            f, g = Gauss_QF(3,1,332444), Gauss_QF(3,1,332444)
            h = f.compose(f)
            print(h)
                >> A forma quadrática é (9,7,110820) e é interpretada
                    como: 9x^2+14xy+110820y^2
        """
        if not isinstance(other, self.__class__):
            raise TypeError("Só podemos compor formas quadráticas")
        if not self.discriminant < 0 or not other.discriminant < 0:
            raise TypeError("Só podemos compor formas "+ \
                            "com discriminante negativo")
        if self.a > other.a:
            return other.compose(self)
        s = self.b + other.b
        n = 2*other.b - s
        if other.a % self.a == 0:
            y_1, d = 0, self.a
        else:
            y_1 = gcdxy(other.a, self.a)[1]
            d = gcdxy(other.a, self.a)[0]
        if s % d == 0:
            y_2, x_2, d_1 = -1, 0, d
        else:
            d_1 = gcdxy(s,d)[0]
```

```
            x_2 = gcdxy(s,d)[1]
            y_2 = -gcdxy(s,d)[2]
        v_1 = int(self.a/d_1)
        v_2 = int(other.a/d_1)
        r = (y_1*y_2*n - x_2*(other.c))%(v_1)
        b_3 = 2*(other.b + v_2*r)
        a_3 = v_1*v_2
        c_3 = int((b_3**2 - 4*self.determinant)/(4*a_3))
        composed = self.__class__(a_3, int(b_3/2), c_3)
        return composed
```

D.3 Sugestão de uso

D.3.1 Princípio

Após a primeira vez que usemos este código, sempre que o quisermos executar, será necessário abrir um terminal na pasta com o caminho `%pastaAnterior%` , ou seja, na pasta que contém `Gauss_QF` e ativar o ambiente virtual usando o comando já visto:

```
.\gauss\Scripts\activate
```

Por fim, podemos usar o comando `py` ou o comando `python` para executar o Python. Agora dependerá das nossas intenções:

1. Caso queiramos efetuar cálculos usando formas quadráticas, ou seja, usar as funções programadas em `Gauss_QF.py`, será necessário escrever

   ```
   from Gauss_QF import Gauss_QF
   ```

2. Caso queiramos usar alguma das funções diversas, ou seja, usar as funções programadas em `primos_div.py`, será necessário escrever

   ```
   from Gauss_QF.primos_div import prod, divm, prime_lst
   ```

   Se não quisermos usar as funções todas, basta apenas escrever as que desejamos.

3. Caso queiramos aceder às funções auxiliares programadas em `_GaussUtils.py`, como por exemplo a função `gcdxy`, basta escrever

   ```
   from Gauss_QF._GaussUtils import gcdxy
   ```

   É claro que, no caso de querer usar outras funções, basta escrever os seus nomes em vez de `gcdxy`.

Caso o utilizador tenha dúvidas sobre o uso de alguma função, após a sua importação, basta digitar, por exemplo

```
help(func)
```

sendo que `func` é o nome da função importada.

Após usar o código, basta sair do Python com o comando `exit()` e para desativar o ambiente virtual, digitamos `deactivate`.

D.3.2 Exemplos de uso

Cálculo do determinante de uma forma quadrática

Neste exemplo, vamos calcular o determinante da forma quadrática $3x^2 + 2xy + 332444y^2$.

```
>>>from Gauss_QF import Gauss_QF
>>>f = Gauss_QF(3,1,332444)
>>>f.determinant
-997331 #Esta é a resposta
```

Formas quadráticas com determinante positivo

Neste exemplo, vamos calcular o período da forma quadrática $2x^2 + 10xy + 4y^2$. Primeiro averiguamos se o seu determinante é positivo e em seguida tentamos executar o cálculo.

```
>>>from Gauss_QF import Gauss_QF
>>>f = Gauss_QF(2,5,4)
>>>f.determinant
17 # A nossa forma quadrática tem determinante 17, é positivo
>>>f.period()
[[(2,5,4),(4,3,-2)],
[(4,3,-2),(-2,3,4),(4,1,-4),(-4,3,2),(2,3,-4),(-4,1,4)]]
# A primeira lista mostra o processo de redução da primeira forma
# quadrática. A segunda lista mostra o seu período.
```

Cálculo da composição de duas formas quadráticas com determinante negativo

```
>>> from Gauss_QF import Gauss_QF
>>> f = Gauss_QF(3,1,332444)
>>> g = f.compose(f)
# Esta linha cria o objeto correspondente à forma quadrática f^2.
# Para sabermos qual é o resultado, é necessário escrever algo como
>>> g.rep_tuple
(9,7,110820)
```

Cálculo do máximo divisor comum entre dois números

```
>>> from Gauss_QF._GaussUtils import gcdxy
>>> gcdxy(15,18)
(3,-1,1)
# Ou seja, 3 é o máximo divisor comum
# Também: 3 = 15*(-1) + 18*1
```

Cálculo da percentagem de números sem fatores primos menores que um limite superior

As próximas linhas ilustram como se usaram as duas funções anteriores para executar o cálculo da subsecção 5.4.

```
>>> from Gauss_QF.primos_div import prod, prime_lst
>>> lim_sup = 139 # O utilizador pode editar este limite
>>> lst = prime_lst(lim_sup)
# Calculo da lista de primos até ao limite superior
>>> C = [(i-1)/i for i in prime_lst(lim_sup)]
>>> result = prod(C)*100
>>> print("Há {} % de números sem fatores até {}".format(result, lim_sup))
```

D.4 Comandos para execução em Linux e iOS

Nesta secção mostramos como adaptar o procedimento que vimos feito para o sistema operativo *Windows*. Algo uniforme a ambos os sistemas operativos *Linux* e *iOS* é que, se a instalação do Python estiver incluida numa distribuição como o Anaconda, ao contrário do Windows, podemos escrever todos os comandos diretamente num `terminal`.

D.4.1 Sistema operativo *Linux*

A execução em Linux é semelhante ao uso em Windows, será necessário apenas ajustar comandos. Para abrir um terminal na pasta desejada (no nosso caso, `%pastaAnterior%`) , abrimos um terminal e digitamos no mesmo o comando

```
cd %pastaAnterior%
```

Eis as adaptações:

- Para criar um ambiente virtual chamado 'gauss': `python3 -m venv gauss`
- Para ativar um ambiente virtual: `source gauss/bin/activate`
- Para instalar o numpy, primeiro instalamos o pip e só depois o numpy.
  - Instalação do pip: `sudo apt install python3-pip`
  - Instalação do numpy: `pip3 install numpy`
- Para executar o Python: `python`

D.4.2 Sistema operativo *iOS*

A execução em iOS é semelhante ao uso em Windows, será necessário apenas ajustar comandos. Para abrir um terminal na pasta desejada, abrimos um terminal e digitamos no mesmo o comando

```
cd %pastaAnterior%
```

No entanto, também é possível abrir diretamente um terminal na pasta desejada (no nosso caso, `%pastaAnterior%`) se o utilizador fizer um clique direito na pasta e selecionar "Open Terminal at Folder" ou equivalente. Eis as adaptações:

- Para criar um ambiente virtual chamado 'gauss': `python3 -m venv gauss`
- Para ativar o ambiente virtual criado: `source gauss/bin/activate`
- Para instalar o numpy, será necessário instalar o pip e só depois o numpy.
  - Instalação do pip:
    1. `curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py`
    2. `python3 get-pip.py`
  - Instalação do numpy: `pip install numpy`
- Para executar o Python: `python`.

Anexo E

Disquisitiones Arithmeticae: O Livro

Poderíamos dizer que, mais do que um livro, o *Disquisitiones Arithmeticae* é uma obra que desencadeia um movimento apenas equiparável ao desencadeado pela obra *Elementos* de Euclides, usado nas escolas até ao século XX. Apresentamos, de seguida, o panorama matemático anterior à sua publicação, baseando-nos nas obras [Wei84] e [Dic52].

E.1 Primordios: Euclides

Paradoxalmente, a Teoria dos Números é tão antiga como recente. Por alturas de 300 a.C., esta disciplina teve a sua génese com o reputado livro *Elementos* de Euclides.

É bastante provável que o seu conteúdo seja anterior, ainda que seja difícil recuperar a sua história. Propriedades de divisibilidade já deveriam ser conhecidas pelos Babilónios e talvez tenham alguma conexão com a irracionalidade de raízes quadradas como $\sqrt{2}$ e $\sqrt{5}$. Os conceitos de 'número primo', 'divisor' e 'múltiplo comum' deverão também ser-lhe anteriores, a avaliar pelos indícios de conhecimento sobre a fatorização de inteiros na Academia de Platão, precedendo os *Elementos* em 70 anos. Ainda assim, foi uma peça fulcral para a disseminação destes conhecimentos.

Nesta obra de 13 Livros, os Livros 7 a 10 são os reservados à Teoria dos Números.

No Livro 7, podemos encontrar uma lista de definições como designadamente as definições de 'unidade', 'número primo', 'número composto', 'número quadrado'. Estabelece sobretudo teoria ainda hoje relevante, a saber:

1. As propriedades da relação de divisão
2. Um algoritmo para encontrar o maior divisor comum entre dois números, atualmente intitulado "algoritmo de Euclides"
3. O "lema de Euclides": se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$. Este lema encontra-se espelhado na definição de elementos primos.

Do mesmo modo, é possível encontrar nos subsequentes Livros a prova da infinidade dos números primos e ainda o que viria a ser considerado o "Teorema Fundamental da Aritmética".

No Livro 10, desenvolve-se um estudo sobre o que ficou conhecido por 'ternos pitagóricos': trios de números naturais a, b, c tais que $a^2 + b^2 = c^2$ e uma maneira de os gerar a todos:

$$a = d(2pq0), \qquad b = d(p^2 - q^2), \qquad c = d(p^2 + q^2),$$

supondo que p, q não têm fatores em comum, a sua diferença é ímpar, $p > q$, e d é o máximo divisor comum entre a, b, c.

Este processo já deveria ser conhecido na Mesopotâmia, mas é Euclides quem o demonstra. No entanto, a coroa de glória dos *Elementos* é, na ótica do seu autor, o enunciado de uma fórmula que gera números perfeitos, números que são soma de todos os seus divisores menores que o número original. Passados 2000 anos, Euler demonstra que todos os números perfeitos pares satisfaziam esta fórmula.

Ainda assim, os Livros 7 a 10 aparecem depois de seis Livros exclusivamente dedicados à geometria de figuras planas, mas antes de três Livros dedicados à geometria de sólidos. Seriam quase um ponto de desconexão se o enunciado destas definições e proposições não viesse quase sempre acompanhado de expressões como 'medir' e se Euclides não tivesse definido a segunda e a terceira potências, como 'números quadrados' e 'números cúbicos', respetivamente.

Em conclusão, temos os primórdios de uma teoria frutífera e relevante nos dias de hoje, mas ainda vista como parte da geometria e não como área autónoma.

E.2 Milénios em construção

E.2.1 Proto-história

Mesmo com a publicação de um manual como os *Elementos*, é necessário ter presente que a Teoria dos Números demorou a levantar voo.

Antes de Euclides, pouco resta da matemática babilónica nesta área. Descobriu-se a tabela de ternos pitagóricos Plimpton 322, eventualmente elaborada entre 1900 - 1600 a.C, o que antecede os *Elementos* de Euclides em mais de 1000 anos.

Para além de Euclides, na Grécia, há ainda que mencionar o interesse por 'números figurados', isto é, números naturais com os quais poderíamos dispor objetos em formas de polígonos regulares, como triângulos, quadrados, pentágonos, entre outros, o que levou à dedução de fórmulas para somar progressões aritméticas como $\sum_{n=1}^{N} n$ e $\sum_{n=1}^{N} n^2$.

Em particular, somos conduzidos a Nicómaco de Gerasa (60 d.C. - 120 d.C.), responsável por calcular a soma dos primeiros números cúbicos e deduzir uma fórmula para o efeito. No seu livro *Introdução à Aritmética* dividiu os números pares em 'abundantes', 'deficientes' e 'perfeitos'; ademais, afirmou que a fórmula de Euclides gerará todos os números perfeitos sem exceção, ainda que não o tenha demonstrado[1].

Pela mesma altura, Diofanto lançava o seu livro *Arithmetica*, uma obra que trata da resolução de equações lineares 'determinadas' e 'indeterminadas' e também de equações quadráticas.

Nesta obra, Diofanto busca soluções racionais, mas faz referência a decomposições de números como soma de quadrados, por exemplo $65 = 4^2 + 7^2 = 1^2 + 8^2$, notando para o efeito

[1] Euler tratou de o fazer.

> *"É da natureza do* 65 *poder ser escrito de duas formas diferentes como soma de dois quadrados, nomeadamente* $16+49$ *e* $64+1$*; tal é o caso, pois é o produto de* 13 *e* 5*, sendo que cada um é a soma de dois quadrados."* ([Wei84], p.11)[2].

Esta justificação demonstra possível conhecimento da identidade:

$$(x^2+y^2)(z^2+t^2) = (xz \pm yt)^2 + (xt \mp yz)^2. \tag{E.1}$$

Diofanto também revela conhecer o processo de Euclides para construir ternos pitagóricos, dando-lhe o nome técnico "enformar".

A identidade supramencionada figura igualmente nos trabalhos de Brahmagupta (598 d.C. - 668 d.C.), que demonstrou as seguintes identidades mais gerais, presentes no lema 1.46:

$$(x^2-Ny^2)(z^2-Nt^2) = (xz \pm Nyt)^2 - N(xt \pm yz)^2, \tag{E.2}$$

$$(x^2+Ny^2)(z^2+Nt^2) = (xz \pm Nyt)^2 + N(xt \mp yz)^2. \tag{E.3}$$

Estas identidades aparecem relacionadas das suas investigações às soluções da equação $x^2-Ny^2 = 1$. O seu método atingiu a plenitude no séc. XII com os trabalhos de Bhāskara (1114 d.C – 1185 d.C), cunhando o método Chakravala ('método cíclico').

Ainda na Índia, basta notar que um século antes de Brahmagupta, Aryabhata (476 – 550), na sua obra *Āryabhatīya*, redescobriu o "algoritmo de Euclides", e transmitiu o que viria a ser conhecido por "Teorema Chinês dos Restos".

Os trabalhos matemáticos da Índia chegaram à Europa através de traduções feitas por matemáticos árabes do séc. X, e acabaram por ser retraduzidos para o Latim no séc. XII. Na mesma altura que Leonardo Pisano (c. 1170 d.C. – c. 1240–50 d.C.), também conhecido como Fibonacci, publicou a obra *Liber Abaci*, em que popularizou o sistema de numeração indo-árabe e os números que seriam batizados com o seu nome.

No entanto, publicou também uma obra menos conhecida intitulada *Liber Quadratorum* que incidia em problemas relacionados com números quadrados em progressão aritmética, em que a identidade de Diofanto figurava uma vez mais, acompanhada de uma prova.

Os trabalhos em Teoria dos Números continuavam esparsos. Depois das publicações de Fibonacci, o século XV assistiu ao nascimento da álgebra simbólica pelas mãos de François Viète, o qual demonstrou a identidade de Diofanto por métodos geométricos. Este matemático generalizou-a usando funções trigonométricas, o que faz com que saísse do âmbito da Teoria dos Números, pois transcendia os números inteiros.

O nascimento da moderna Teoria dos Números terá ocorrido um pouco mais tarde, catalizado pela tradução, para Latim, da obra *Arithmetica* de Diofanto por Claude Gaspar Bachet em 1621.

E.2.2 Fermat: o 'Príncipe dos Amadores'

Pierre de Fermat (1607 d.C. - 1665 d.C.), conhecido como 'Príncipe dos Amadores', era advogado de profissão, trabalhando em matemática por mero divertimento.

[2] "It is in the nature of 65 that it can be written in two different ways as a sum of two squares, viz., as $16+49$ and as $64+1$; this happens because it is the product of 13 and 5, each of which is a sum of two squares."

A correspondência de Fermat permite concluir que começou a trabalhar em Teoria dos Números por volta de 1636, quando não possuía mais que a versão de Bachet de *Arithmetica*, e a apresentação de parte da mesma obra em *Zetètica*, de François Viète, de 1593. Não considerava estes trabalhos próprios de Teoria dos Números, já que afirmou no seu desafio de 1657 que a Teoria dos Números tratava de números inteiros.

Trabalhos desenvolvidos em Teoria dos Números:

1. O 'teorema de Natal de Fermat', em que conclui que apenas os primos da forma $4k + 1$ podem ser escritos como soma de dois quadrados.

2. Critérios para a representação de primos em expressões como $x^2 + 2y^2$ e $x^2 + 3y^2$.

3. Popularização da equação de Pell $x^2 - Ny^2 = 1$ em 1657, lançando um desafio aos matemáticos da época com a sua resolução em números inteiros.

4. Criação do método da 'descida infinita', uma variante da redução ao absurdo.

5. O 'pequeno teorema de Fermat', em que afirma que se p é primo, então p divide o número $a^p - a$ para qualquer inteiro a.

6. O 'último teorema de Fermat', o qual afirma que a equação $x^n + y^n = z^n$ não tem soluções inteiras não triviais para $n > 2$. Este teorema foi apresentado sem uma demonstração, dando assim dores de cabeça a gerações inteiras de matemáticos.

No entanto, grande parte das suas proposições foram formuladas sem demonstração, o que não era incomum, dada a política de secretismo em vários círculos científicos da época.

Fermat morreu em 1665, sem trabalhos publicados em seu nome, apenas com correspondência trocada com vários matemáticos influentes.

Em 1670, o seu filho Samuel voltou a publicar a obra de Diofanto já referida com as anotações e comentários feitos pelo pai, bem como um ensaio particular de Fermat e várias cartas de conteúdo aritmético. O interesse em Teoria dos Números voltou a esfumar-se, mas desta feita por menos tempo.

Avançando mais uns anos, chegamos a um outro matemático: Leonhard Euler.

E.2.3 Euler: um catalizador

Leonhard Euler (1707 d.C. - 1783 d.C.) foi um matemático suíço, um dos mais profícuos, tendo fundado áreas como a Teoria de Grafos e passando por disciplinas tão diversas como o Cálculo Infinitésimal, a Topologia, Álgebra, entre outras. Em 1729, quando vivia em São Petersburgo como adjunto da recém-fundada Academia das Ciências, foi atraído para a área da Teoria dos Números quando o seu amigo Christian Goldbach lhe indicou os trabalhos feitos por Fermat. A partir deste momento, o interesse por esta área não mais se desvaneceu. Euler dedicou-se a completar as lacunas deixadas por Fermat e a apresentar a demonstração de várias proposições antes não demonstradas.

Euler continuou também o trabalho deixado por Fermat e estudou os critérios de representação de números primos como $x^2 + Ny^2$, fundando aquilo que se poderia chamar 'formas

quadráticas'. Correspondendo-se com Goldbach, em 1742 enuncia como conjetura o que seria conhecido como a "Lei da Reciprocidade Quadrática".

É na Teoria Analítica dos Números que deixa uma marca importante pelo seu trabalho em partições, na soma de quatro quadrados, séries numéricas e na distribuição de números primos, contexto em que podemos destacar o que hoje se conhece como 'função zeta de Riemann'.

Fica a dever-se a este matemático o "mau batismo" da equação $x^2 - Ny^2 = 1$ como 'Equação de Pell'. (Note-se que ao escrever sobre a ligação entre frações continuadas e respetivas soluções, equivocou-se quanto à autoria da sua resolução.)

E.2.4 Lagrange: uma continuação

Contemporâneo de Euler, Joseph-Louis Lagrange (1736 d.C. - 1813 d.C.) também prestou o seu contributo matemático sobretudo na área da Análise Matemática, Mecânica Celeste e Teoria dos Números. Relativamente a esta última, eis alguns exemplos dos seus trabalhos:

1. A resolução definitiva da equação de Pell, provando que $x^2 - Ny^2 = 1$ tem soluções não triviais para qualquer N número natural não-quadrado.

2. A primeira demonstração do teorema de Wilson: p é primo se e só se $(p-1)!+1$ é múltiplo de p.

3. Demonstração de que todo o número inteiro se escreve como soma de quatro quadrados.

4. A demonstração de mais alguns dos resultados enunciados por Fermat.

5. Estudo das 'formas quadráticas binárias' $ax^2 + bxy + cy^2$ e tratamento do problema da representação de números inteiros segundo estas expressões na sua obra *Recherches d'Arithmetique*, de 1775, generalizando assim o trabalho de Euler e Fermat em equações como $x^2 + Ny^2$.

E.2.5 Legendre: uma centelha

Adrien-Marie Legendre (1752 d.C. – 1833 d.C.) foi importantíssimo para a Teoria dos Números. Seguidor do trabalho de Euler e de Lagrange, em 1798 escreveu a obra *Essai sur la théorie des nombres* numa tentativa de mostrar o estado corrente da Teoria dos Números.

O trabalho deste matemático deu seguimento aos trabalhos desenvolvidos sobre as formas quadráticas binárias. É o primeiro a publicar uma demonstração da "Lei da Reciprocidade Quadrática", introduzindo, para o efeito, o símbolo com o seu nome, ainda que esta demonstração se baseasse em resultados não demonstrados.

Em vários aspetos, o seu trabalho viria a coincidir com o trabalho de Gauss.

Conjeturou o "Teorema dos Números Primos", demonstrado de forma independente por Jacques Hadamard e por Charles-Jean de la Vallée-Poussin quase cem anos depois.

No entanto, nesta altura, não obstante a atividade desenvolvida, a Teoria dos Números mantinha-se uma disciplina incipiente, sem um fio condutor, uma coleção de resultados diversos e técnicas dispersas.

Porém, em 1801 assiste-se à publicação do livro que mudou esta área definitivamente, *Disquisitiones Arithmeticae*.

E.3 Disquisitiones Arithmeticae

E.3.1 Gauss: O 'Príncipe da Matemática'

O contributo de Gauss para a Matemática é inegável, sendo-o ainda mais para a Teoria dos Números, disciplina que contribuiu para consolidar.

Johann Friedrich Carl Gauss, mais conhecido por Carl Friedrich Gauss, nasceu em 30 de Abril de 1777 d.C., em Brunswick. Filho de Gebhard Dietrich Gauss e de Dorothea Benze, era de origem humilde, e nenhum dos pais possuía educação formal.

O seu talento foi descoberto por um professor primário, Büttner, o qual contribuiu para que Gauss pudesse frequentar o ensino secundário.

Foi já perto da conclusão do ensino secundário que o talento de Gauss chegou aos ouvidos do duque de Brunswick. Impressionado com o jovem Carl, o duque atribuiu-lhe uma quantia anual, para que pudesse prosseguir os estudos.

Entre 1792 e 1795, estudou no Collegium Carolinum, onde se familiarizou com literatura matemática clássica e aprendeu línguas clássicas como o Latim, e ainda filosofia e matemática superior.

Concluído este ciclo de estudos, Gauss troca Brunswick por Göttingen e frequenta a Universidade Georgia Augusta por mais três anos. É nesta universidade que dá início à elaboração de *Disquisitiones Arithmeticae*, o seu *magnum opus*. Deixa a universidade em 1798, sem obter qualquer diploma da instituição.

E.3.2 *Disquisitiones Arithmeticae*

Disquitiones Arithmeticae é uma coletânea dos resultados anteriores publicados até à época, mas também da sua própria investigação, muitas vezes continuando o trabalho começado pelos matemáticos acima citados. A tradução do seu título para português seria algo como "Indagações Aritméticas".

Analisando o seu diário, Gauss terá começado a dedicar-se a investigações aritméticas por sua conta em 1792, tinha então 15 anos; em 1796, já tinha provas de temas tão complexos como a Lei da Reciprocidade Quadrática e a 'Construtibilidade do Heptadecágono'; em 1797, teria já dado forma a um primeiro manuscrito do livro, que enviaria para impressão em 1798. Dificuldades técnicas por parte do responsável pela impressão levaram a que a publicação demorasse três anos, tempo que Gauss usou para expandir o manuscrito com novos resultados, especialmente no Capítulo 5. Em 1801, estava impressa a obra, tinha então Gauss 24 anos.

A monumentalidade desta obra advém de fatores vários, entre os quais se poderia mencionar a jovem idade do seu autor, a inovação ilustrada nos seus conceitos, notação e resultados, e o engenho e subtileza presentes nas suas provas. Tudo isto contribuiu para que a Teoria dos Números deixasse de ser uma coleção de resultados dispersos e técnicas soltas, e pudesse ser elevada a uma disciplina autónoma.

A obra *Disquisitiones Arithmeticae* está dividido em sete secções[3]:

1. Da Congruência dos Números em Geral.[4]
2. Congruências do Primeiro Grau.[5]
3. Sobre os Resíduos das Potências.[6]
4. Sobre as Congruências do Segundo Grau.[7]
5. Sobre as Formas e as Equações Indeterminadas de Segundo Grau.[8]
6. Aplicações Várias das Investigações Precedentes.[9]
7. Equações que Definem Secções de um Círculo.[10]

As primeiras três secções são breves, introdutórias e visam rever resultados previamente conhecidos, nomeadamente o 'pequeno teorema de Fermat', o 'teorema de Wilson', bem como confirmar a existência de raízes primitivas.

Na Secção 4, Gauss começa a aditar as suas investigações pessoais. O objetivo da secção é demonstrar a "Lei da Reciprocidade Quadrática", dando, assim, a primeira demonstração correta. A prova é extensa; para o efeito, Gauss divide a demonstração em oito casos diferentes. A demonstração em causa vem acompanhada de referências aos anteriores trabalhos de Fermat, Euler, Lagrange e Legendre na área.

A Secção 5 constitui o âmago do livro. Gauss dedica-a às expressões do tipo $F = ax^2 + 2bxy + cy^2$, o que ficara conhecido como formas quadráticas binárias. Parte do material desta secção não é original, pois já tinha sido desenvolvido por Lagrange; porém, Gauss é capaz de unificar os resultados previamente obtidos. O problema central é determinar que números inteiros M poderiam ser representados por estas expressões, mas Gauss também é capaz de resolver o problema inverso, isto é, conhecendo M, a, b, c, quais seriam os valores de x e y.

A Secção 6 apresenta várias aplicações de toda a teoria desenvolvida até ao momento, como a decomposição em frações parciais, o que viria a ser útil para a integração de funções racionais. É esta a secção mais relevante para a presente dissertação, já que os testes de primalidade a estudar se encontram no final da mesma.

A Secção 7 é a mais popular, porquanto apresenta uma condição necessária para a construção de polígonos regulares, resolvendo um problema em aberto desde a Antiguidade Grega.

[3]Traduzimos os títulos com base na tradução da mesma obra em língua castelhana.
[4]Em latim: Sectio prima. De numerorum congruentia in genere.
[5]Em latim: Sectio secunda. De congruentiis primi gradus.
[6]Em latim: Sectio tertia. De residuis potestatum.
[7]Em latim: Sectio quarta. De congruentiis secundi gradus.
[8]Em latim: Sectio quinta. De formis aequationibusque indeterminatis secundi gradus
[9]Em latim: Sectio sexta. Variae applicationes disquisitionum praecedentium.
[10]Em latim: Sectio septima. De aequationibus, circuli sectiones definientibus.

E.3.3 O impacto

Como referido no Capítulo I, este livro abarca todo um movimento. Muito poderia ser dito sobre a obra; depois da publicação de *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae* - livro dedicado ao DA escrito e editado por Goldstein, Schappacher, Schwermer, três distinguidos historiadores matemáticos - muito pouco poderia ser acrescentado.

Nesta medida, não querendo negar a abordagem eminentemente histórica desta dissertação, nesta subsecção procurarei fazer uma síntese do alcance desta obra baseando-me, para o efeito, no livro supracitado ([GSS07]) e na obra *A History of Abstract Algebra*, de Jeremy Gray ([Gra18]).

Após a história conturbada da obra, o DA acabou por ser publicado em 1801. Em França, foi amplamente bem recebido. Um ano mais tarde, Adrien-Marie Legendre menciona o livro na Academia Francesa.

> *"O cidadão Legendre comunica uma descoberta geométrica feita na Alemanha por M. Charles Frédéric Bruce [sic], de Brunswick, e por si publicada no seu livro Disquisitiones Arithmeticae, Leipzig,* 1801*"* ([GSS07], p.19).[11]

O projeto de tradução francesa foi impulsionado pelo matemático mais proeminente da época, Pierre-Simeon Laplace, e, em 1804, Lagrange escreve a Gauss:

> *"As vossas Disquisitiones elevaram-vos rapidamente à categoria dos principais matemáticos e considero que a última secção contém a mais bela descoberta analítica que foi realizada desde há muito tempo."*([Ruf17], p. 56).[12]

Esta citação é importante, pois revela a receção positiva do livro por parte de um dos maiores matemáticos da época como o era Lagrange, mas também porque revela o estado de desenvolvimento da Teoria dos Números na época. As descobertas de Gauss constantes da Secção 7 que associam a resolução de equações como $x^n - 1 = 0$ à geometria são vistas como "analíticas", já que a Teoria dos Números (e a Matemática Pura no geral) era vista como um tema secundário em comparação com a Física Matemática e a Astronomia.

Pelo *Disquisitiones Arithmeticae* passaram, sobretudo, dois tipos de matemáticos.

Do primeiro tipo, há que salientar matemáticos como Augustin-Louis Cauchy, que em muito beneficiaram do livro, porém, esta obra terá representado uma parte secundária da sua carreira.

No caso de Cauchy, tal é notório, pois em 1812 usou conceitos diretamente extraídos do DA, como a noção de determinante para desenvolver a sua Teoria de Combinações e Determinantes, fulcral para o nascimento da Teoria de Grupos.

Do segundo tipo, refiram-se os matemáticos que sempre tiveram uma presença secundária na comunidade matemática, dos quais poderíamos citar Sophie Germain.

No caso de Sophie Germain, esta demonstra ter um conhecimento aprofundado de todas as secções do livro, desde a Secção 1 *Da Congruência dos Números em Geral* na qual usa as congruências para os seus trabalhos no "Último Teorema de Fermat" até à densa Secção 5, *Sobre as Formas e as Equações Indeterminadas de Segundo Grau*, da qual revela ter conhecimentos sobre a composição de formas quadráticas binárias.

[11] No original: "Citizen Legendre communicates a geometrical discovery, made in Germany by M. Charles Frédéric Bruce [sic], from Brunswick, and published by him in his work entitled Disquisitiones arithmeticae, Leipsik, 1801"

[12] No original: "Vos Disquisitiones vous ont mis tout de suite au rang des premiers géomètres et je regarde la dernière section comme contenant la plus belle découverte analytique qui ait été faite depuis longtemps."

Em suma, o DA foi recurso utilizado por, pelo menos, duas diferentes maneiras, parcialmente ou integralmente, dependendo do matemático.

Nos primeiros tempos, importa referir que foi a resolução da equação ciclotómica $x^n - 1 = 0$ que tornou o livro conhecido. Aparecendo em trabalhos vários como o de Barlow no seu tratado sobre a família de soluções de equações indeterminadas, Lobachevsky publica uma nota sobre o assunto, Charles Babbage recomenda o livro numa lista restrita de livros dirigida aos membros da recém-fundada "Cambridge Analytical Society", fazendo particular referência ao teorema especial formulado por Gauss sobre a resolução da equação $x^n - 1 = 0$.

Por consequência, durante muitos anos considerou-se a Teoria dos Números um ramo da Análise, e ainda que Gauss tivesse declarado, no início da sua obra, que os seus trabalhos diriam exclusivamente respeito aos números inteiros, posições como a de Legendre (*"Não distinguirei entre a Teoria de Números e a Análise de Indeterminadas e considerarei estas disciplinas como ramos da Análise Algébrica"*([GSS07], p.22)[13]) prevaleceram. Por seu turno, Legendre não usou a notação de Gauss para as congruências, nem as considerava um assunto necessário.

Deste modo, é necessário destacar que o impacto dos trabalhos de Gauss na Teoria dos Números nos primeiros anos incidiu sobretudo na Análise, pois foi o seu teorema constante da última secção que mobilizou toda a comunidade matemática.

[13]No original: "I shall not distinguish the Theory of Numbers from Indeterminate Analysis, and I consider these two parts as making up one single branch of Algebraic Analysis."